Namely, Painless: A unifying approach to safe programming with first-order syntax with binders
Nicolas Pouillard

To cite this version:

HAL Id: tel-00759059
https://tel.archives-ouvertes.fr/tel-00759059
Submitted on 1 Dec 2012

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Une approche unifiante pour programmer sûrement avec de la syntaxe du premier ordre contenant des lieurs

english title: Namely, Painless

A unifying approach to safe programming with first-order syntax with binders

Nicolas Pouillard
À mon papa...
Abstract

This dissertation describes a novel approach to safe metaprogramming. A meta-program is a program which processes programs or similar data. Compilers and theorem provers are prime examples of meta-programs which could benefit from this approach. To this end, this work focuses on the representation of names and binders in data structures.

Programming errors are really easy to make with usual techniques. We propose an abstract interface to names and binders that rules out these errors. This interface is implemented as a library in Agda. It allows defining and manipulating term representations in nominal style. Thanks to abstraction, other styles are supported as well: the de Bruijn style, the combinations of these styles, and more.

Whereas indexing the types of names and terms with a natural number is a well-known technique to better control de Bruijn indices, we index them with worlds. Worlds are at the same time more precise and more abstract than natural numbers. Via logical relations and parametricity, we are able to demonstrate in what sense our library is safe, and to obtain theorems for free about world-polymorphic functions. For instance, we prove that a world-polymorphic term transformation function must commute with any renaming of the free variables. The proof is entirely carried out in Agda.

The usability of our technique is shown on several examples including normalization by evaluation which is known to be challenging. We show that our world-indexed approach can express a wide range of data types by embedding several definition languages from the literature.
Résumené

Cette thèse décrit une nouvelle approche pour la métaprogrammation sûre. Un méta-programme est un programme qui manipule des programmes ou assimilés. Les compilateurs et systèmes de preuves sont de bons exemples de méta-programmes qui bénéficieraient de cette approche. Dans ce but, ce travail se concentre sur la représentation des noms et des lieux dans les structures de données.

Les erreurs de programmation étant courantes avec les techniques usuelles, nous proposons une interface abstraite pour les noms et les lieux qui élimine ces erreurs. Cette interface est implémentée sous forme d’une bibliothèque en Agda. Elle permet de définir et manipuler des représentations de termes dans le style nominal. Grâce à l’abstraction, d’autres styles sont aussi disponibles : le style de De Bruijn, les combinaisons de ces styles, et d’autres encore.

Nous indiquons les noms et les termes par des mondes. Les mondes sont en même temps précis et abstraits. Via les relations logiques et la paramétricité, nous pouvons démontrer dans quel sens notre bibliothèque est sûre, et obtenir des “théorèmes gratuits” à propos des fonctions monde-polymorphiques. Ainsi une fonction monde-polymorphique de transformation de termes doit commuter avec n’importe quel renommage des variables libres. La preuve est entièrement conduite en Agda.

Notre technique se montre utile sur plusieurs exemples, dont la normalisation par évaluation qui est connue pour être un défi. Nous montrons que notre approche indiquée par des mondes permet d’exprimer un large panel de type de données grâce à des langages de définition embarqués.
Remerciements

Trois années de noms et de termes. Des liens puis des noms, des noms et des indices, puis des indices seulement, puis finalement encore des noms. Aujourd’hui j’écris ces remerciements et ce sont vos noms qui me viennent à l’esprit.

Je porte mes remerciements tout d’abord à ma famille, mes parents, pour m’avoir soutenu dans mes longues études. Merci aussi à mon épouse, Gaëlle, qui m’a non seulement soutenu mais épaulé, écouté, poussé, aidé, ... Bref, elle est aussi responsable de cet aboutissement.

Je tiens particulièrement à remercier mes relecteurs pour leur travail remarquable. Leurs relectures de ce document m’ont permis de nombreuses améliorations rendant le présent document plus accessible et plus complet.

Je remercie le LRDE qui m’a aiguillé vers la recherche, je remercie en particulier Akim Demaille pour son cours de compilation qui m’a initié à la conception de langages.

Je remercie d’avance tous ceux que je ne mentionne pas individuellement ici : membres de ma famille, camarades, collègues, ami(e)s, simples connaissances. Vous qui justement lisez ces lignes, je vous en remercie.

Un grand merci à toute l’équipe Gallium de l’INRIA Rocquencourt et tous les membres que j’y ai rencontrés. Cette équipe m’a accueilli jeune ingénieur et m’a rendu jeune chercheur. Plus particulièrement je remercie : Michel Mauny pour m’avoir accepté en stage mais aussi sur le contrat qui a suivi ; j’y ai appris une foule d’anecdotes sur l’évolution des dialectes succés-sifs de Caml ; grâce à lui et malgré lui j’ai appris à apprécier la programmation paresseuse (sans jeux de mots) ce qui m’a ouvert de nouveaux horizons. Puis c’est au tour de François Pottier, qui m’a accepté en thèse et m’a habilement guidé et soutenu pendant ces années. Il a su être disponible et à l’écoute. Outre une montagne de connaissances scientifiques, j’ai appris de lui l’art d’écire des articles bien que j’ai encore beaucoup à apprendre à ce sujet. Xavier Leroy pour son accueil et sa bienveillance quant à la bonne marche de l’équipe ; Damien Doligez pour son intarissable culture et ses théories sur tout ; Didier Rémy pour ses discussions sur les détails du fonctionnement de \TeX ; Alain Frisch pour m’avoir enseigné tellement de choses sur OCaml et la programmation fonctionnelle en général pendant les mois durant lesquels j’ai partagé son bureau ; Yann Régis-Gianas pour avoir tracé
une voie qu’il m’a suffi d’emprunter ; Berke Durak pour m’avoir accompagné dans le développement d’ocamlbuild ; Benoit Razet pour toutes nos discussions sur les automates et les structures de flots de données ; Gérard Huet pour ses anecdotes variées qui m’ont beaucoup appris ; Jean-Baptiste Tristan pour avoir participé et accueilli chez lui l’équipe des “jeunes” de Gallium au concours ICFP ; Tous ceux qui ont participé aux concours ICFP ; Arthur Chaguéraud pour son secret de l’efficacité : les axiomes Coq et notepad++ ; Zaynah Dargaye, Boris Yakobowski et Paolo Herms pour les discussions et les bons moments passés avec eux ; Benoît Montagu pour m’avoir ouvert son bureau et avoir partagé des discussions fructueuses sur nos thèses respectives ; Julien Cretin pour sa singularité mais aussi pour tous les sujets sur lesquels nous pouvons discuter agréablement ; Alexandre Pilkiewicz de m’avoir trainé jusqu’au parcours sportif un certain nombres de fois ; Jonathan Protzenko car grâce à lui le web évolue de jour en jour :) ; Tahina Ramananandro pour nos discussions politiques et nos concours de jeux de mots fumeux ; Dana Xu pour ses encouragements ; Gabriel Scherer et Valentin Robert pour leurs nombreux commentaires sur des parties de ce document.


J’ai une pensée aussi pour tous les “camarades de navette” avec qui j’ai pu discuter pendant un des nombreux trajets entre Paris et Rocquencourt.

À Jean-Philippe Bernardy, pour avoir rendu la paramétricité accessible et claire dans un cadre simple et élégant. Ses travaux ont amplement aidé les miens en apportant l’outil de preuve adapté à ce problème.
Contents

1 Introduction 13
  1.1 Programs and Programming Languages ....................... 14
  1.2 Program syntax ........................................... 15
  1.3 Typing .................................................. 17
  1.4 Program representation, meta-programming .................. 19
  1.5 Names and local bindings ................................ 23
  1.6 Scoping .................................................. 25
  1.7 Empowering our language .................................. 28

2 The nominal approach 41
  2.1 Introduction to the nominal approach ....................... 41
    2.1.1 Warm-up: the bare nominal approach .................... 41
    2.1.2 Using well-formedness judgements ...................... 44
    2.1.3 Well-scoped terms .................................... 47
  2.2 NomPa: A programming interface in nominal style ........ 48
    2.2.1 All we need to define nominal syntax .................. 50
    2.2.2 Building binders and names ............................ 51
    2.2.3 World widening: Name weakening ....................... 53
    2.2.4 Comparing and refining names .......................... 56

3 Programming on top of NomPa 59
  3.1 Various examples ........................................ 59
    3.1.1 Example: computing free variables ..................... 59
    3.1.2 Example: working with environments .................... 60
    3.1.3 Example: Term comparison ............................. 62
  3.2 Kits and Traversals ..................................... 63
    3.2.1 Traversal Kits ....................................... 63
    3.2.2 Coercing kit ......................................... 64
    3.2.3 Renaming kits ........................................ 65
    3.2.4 Substitution kit ...................................... 67
    3.2.5 Other kits and combinators ............................ 68
    3.2.6 Reusable traversal .................................... 68
    3.2.7 Reusing the traversal ................................. 69
Chapter 1

Introduction

Foreword

This document describes my work during these past three years which has been done under the direction of François Pottier. This work extends the research topic of safe meta-programming by providing a novel approach to the representation of programs with names and binders. – Nicolas Pouillard

Safe meta-programming is a research topic which is part of the broader topic of programming language design. One of the goals of the research in programming language design is to provide programmers with better tools allowing to produce correct software applications in a reasonable amount of time. Since correct software applications (programs for short) are not supposed to crash, language designs have to incorporate safety features to detect programming errors as soon as possible. Modern language designs often come with some static disciplines such as lexical scoping, strong typing and the like. These static disciplines are used to reject the programs we do not want to run.

A program may process various forms of data such as numbers, text, spreadsheets, images, sound, and many more. Some programs process other programs, they are called meta-programs. Meta-programs cover a wide class of programs ranging from compilers, to static analyzers, code generators, etc. Proof systems, proof assistants and theorem provers are also meta-programs since propositions and proofs share the same kind of structure as programs. Moreover since language designs come with static disciplines, we claim that meta-programs should follow these disciplines when processing programs. For instance if a program $A$ written in a programming language $P$ generates a program $B$ written in a programming language $Q$, we want $A$ to follow the static discipline of $P$, moreover we want $B$ which does not exist yet to follow the static discipline of $Q$.

This first chapter aims at introducing all the notions to understand
the research problem that we are focusing on. This chapter requires lit-
tle knowledge in the design of programming languages, but does require
some knowledge about computers, mathematics and programming. Hence
this introduction chapter can be safely skipped by readers accustomed with
the research topic.

1.1 Programs and Programming Languages

To introduce the notions of programs and programming languages, let us
start with an example of a simple program:

\[
\text{print "Hello! 2 times 21 is equal to " >> print (show (2 * 21))}
\]

Most generally, programs are written to be executed on a computer.
Running a program often results in the execution of different tasks and
yields a final result. In our previous example the program is meant to print
on the screen: “Hello! 2 times 21 is equal to 42”. Printing on the
screen is done with the construct called \texttt{print}. This printing construct is
used twice. The two uses are \textit{sequenced} using the construct \texttt{>>}, which
will perform the action on the left and then the action on the right. The
number 42 is computed from the arithmetic expression \texttt{2 * 21} which is then
turned into a printable form using the construct called \texttt{show}.

This program, such as any program, is written in a programming lan-
guage. Programming languages are described by a finite set of constructs,
rules explaining how the constructs can be used and rules giving the be-
behavior of programs. In our further examples the programming language
contains constructs such as \texttt{print}, \texttt{>>}, \texttt{show}, *, character strings such
as “Hello! 2 times 21 is equal to ”, numbers such as 2 and 21, and
parentheses. With these constructs our programming language is not much
better than a simple calculator.

This tiny introductory programming language is built to be a subset
of the \texttt{Agda} language. \texttt{Agda} \cite{Norell:2007} is a total functional pro-
gramming language, based on dependent type theory. \texttt{Agda} is used thoroughly
in this document. First it is used to introduce the research topic of meta-
programming. Second it is used to implement our solution to the problem.
Third it is used to formalize our system and show its soundness. Alas, ad-
vanced languages such as \texttt{Agda} are far from simple to completely describe.
The first set of programming constructs we introduce is roughly common
to most languages and is described simply in great detail. The second set
of constructs follows the development of functional programming languages
(such as \texttt{Haskell}, \texttt{ML}, or \texttt{Lisp}). They are described more quickly and
may require further reading about these topics. An excellent introduction
1.2. PROGRAM SYNTAX

Examples. The following program makes use of the four basic arithmetic operators to compute the value 42. Operators are attributed with their usual semantics, addition is + and multiplication is *. Subtraction and division (\(\div\) and \(\div\)) are restricted to natural numbers, meaning that they return 0 when going out of range.

\[(1 + 1) \ast (28 \div 14 \div 2)\]

The following program illustrates character string literals and their concatenation with ++. This program prints “Hello world!” on the screen:

```
print ("Hello" ++ " " ++ "world!")
```

Our next program illustrates the use of show to turn a number into a character string containing its decimal representation. This program prints “show 1 renders as: 1” on the screen:

```
print ("show 1 renders as: " ++ show 1)
```

The following program illustrates the use of >> to sequence two actions from left to right. This program prints “Print me first.” and then prints “Then print me.” on the screen.

```
print "Print me first." >> print "Then print me."
```

We have lists in our programming language. The simplest list value is the empty list, written []. The following program is a list with three elements, namely "a", "bc" and "5":

```
[ "a" , "b" ++ "c" , show (2 + 3) ]
```

We go from lists to trees by using the construct called node. The first argument of node is the label of the node and the second is the list of children of the node. The following program represents a six-node tree

...
depicted hereafter:

```plaintext
node "A"
  [ node "B" [], node "C" [ node "D" [], node "E" [] ], node "F" [] ]
```

**Syntax of our arithmetic calculator**

The syntax of a programming language describes when a program has a valid “shape”. In particular it does not check if the program has a valid “meaning”. For instance, the program `1 + "Hello!"` has a valid syntax but no valid meaning in our tiny language.

Any non-empty sequence of digits (0, 1, 2, 3, 4, 5, 6, 7, 8, 9) is a valid literal number and a valid program as well. A valid literal character string is a sequence of characters different from the double quote character (""") and surrounded by two double quote characters (we avoid talking about escape sequences because we do not need them here). If two programs `p_1` and `p_2` are syntactically valid, then for any operator • among +, -, *, ÷, ++, >> the program `p_1 • p_2` is syntactically valid. These operators are said to be *infix*, meaning that they appear between the two operands. If `p` is a syntactically valid program, then `print p`, `show p` and `(p)` are syntactically valid. If `p_1`, `p_2`, ..., `p_n` are syntactically valid programs, then `[ p_1 , p_2 , ..., p_n ]` is syntactically valid. Finally if `p_1` and `p_2` are syntactically valid programs then `node p_1 p_2` is syntactically valid.

Of course not every textual program is syntactically valid. Consider this example: `3 + * 4`. This program does not follow the rules we just described, hence it is rejected as syntactically invalid.

Syntax also comprises some details about layout and comments. Spaces and newlines are important to some extent. Spaces or parentheses have to be used to separate the words in a program. However, as long as they are separated, how many spaces or newlines are used to separate two words does not matter. There is special support in the syntax to embed comments in our programs. There are two syntaxes used in our language. A comment can start with `{` and stop with `}` or can start with `--` and stop at the
end of line. Here is a syntactically valid program to illustrate layout and comments:

```plaintext
print "Hello..." >> -- this prints Hello...
print {- extra spaces and comments are ok -} "...world!"
```

1.3 Typing

Typing captures, ahead of time, programs that may go wrong. Typing might be seen as a vigilant companion giving advice on our programs. When typing says that our program is ill-typed, then this is a program we may not want to even try running. If the typing says our program is fine, then we know for sure that the program will not crash.

Such a technology is to be applied systematically before running a program. It is an affordable safety measure which massively helps program development, maintenance, testing, and verification.

However, verifying that a program cannot crash without running it is a difficult problem to say the least. In particular we want the typing part of our system to always terminate, even if the given program does not terminate. We not only want the typing to terminate but to answer if the program is well-typed or not. If so we say that such a type system is decidable.

A type system is said to be **sound** if and only if every well-typed program is a non-crashing program. We expect every well-designed type system to be sound.

A type system is said to be **complete** if and only if every non-crashing program is well-typed. The decidability constraint entails that a type system will never be complete for non-trivial languages. For further reading on the topic of type systems we recommend reading “Types and Programming Languages” [Pierce, 2002] and “Advanced Topics in Types and Programming Languages” [Pierce, 2005].

**Typing our arithmetic language** The first goal of type systems is to prevent us from running programs that may crash. To do so, they define **types**, an abstraction to classify pieces of data. By extension, types also classify programs computing pieces of data. Types help to define a common “contract” for producers and consumers of a piece of data. This kind of “contracts” in on the shape of data. The more shapes are allowed by a type, the weaker the type is. The strength of a type affects producers and consumers in different ways. If a type is weak, it is easy for producers of this type to be well-typed. If a type is strong, the producers have to meet all the constraints imposed by the type. This is the opposite for consumers. If a type is strong, the data has a known precise shape, and the consumer
has an easy job. If a type is weak, then the consumer has to consider all the shapes that the data can take.

To illustrate the notion of typing, we equip our little programming language with such a type discipline. Step by step we introduce new types and how the constructs of our language are typed.

We have only a few types of values. We introduce the type $\mathbb{N}$ as the type of numbers ($0, 1, 2, \ldots$) and of programs computing numbers (such as $2 \times 21$).

Given a type $\tau$ (such as $\mathbb{N}$) and a program $p$ (such as $6 \times 7$), we write $p$ has type $\tau$ to formally assert that the program $p$ is of type $\tau$. We call these type assertions typing judgements. The following paragraphs define the type system for our tiny language by giving a typing judgement for each construct.

For each number $n$, $n$ has type $\mathbb{N}$. Given two programs $p_1$ and $p_2$, if both have type $\mathbb{N}$, then $p_1 + p_2$, $p_1 \times p_2$, $p_1 \div p_2$, and $p_1 \div p_2$ all have type $\mathbb{N}$ as well. For instance with these rules one can formally assert: $6 \times 7$ has type $\mathbb{N}$.

Our second type of basic values is text values. To this end we introduce the type $\text{String}$ as the type of text values such as "Hello!" and of programs computing text values such as "Hello " ++ show 42. More precisely for each syntactically valid text value $s$, $s$ has type $\text{String}$. If two programs $p_1$ and $p_2$ have type $\text{String}$ then the program $p_1 ++ p_2$ has type $\text{String}$ as well. If a program $p$ has type $\mathbb{N}$ then show $p$ has type $\text{String}$.

It is now time to show an ill-typed program: "Hello! " ++ 42. While this program is syntactically valid, it does not follow our typing rules. There is indeed only one rule about the construct ++. This rule imposes programs on each side of ++ to be of type $\text{String}$. While "Hello! " is of type $\text{String}$, 42 is not. The only rule that applies to 42 says that it is of type $\mathbb{N}$. Since $\text{String}$ and $\mathbb{N}$ are different, this program is rejected as being ill-typed.

Our little programming language has list values. However there is no single type for all lists. The type of a list depends on the type of its elements. We require all the elements of a list to have the same type. Given any type $A$, if $p_1, p_2, \ldots, p_n$ are programs of type $A$ then $[ p_1, p_2, \ldots, p_n ]$ is of type $\text{List } A$. Thus there is no single type for lists, but for each type $A$ there is a type for lists where elements are of type $A$, namely $\text{List } A$. For instance $\mathbb{[ } 1, 2 \mathbb{] }$ has type $\text{List } \mathbb{N}$, and $\mathbb{[ [ } 1, 2 \mathbb{], [ 3 ] ]}$ has type $\text{List } (\text{List } \mathbb{N})$.

Our next type is the type of trees. Like for lists, the type of trees is parameterized by the type of its elements, namely the labels of nodes. For each type $A$, $\text{Tree } A$ is the type of trees with labels of type $A$. To build a tree we use the construct node: given a type $A$, if $p_1$ has type $A$ and $p_2$ has type $\text{List } (\text{Tree } A)$ then node $p_1 p_2$ has type $\text{Tree } A$.

The following program has type $\text{Tree String}$:
node "A" [ node "B" [], node "C" [] ]

This one has type Tree N:

node 1 [ node 2 [], node 3 [] ]

This one is ill-typed, though:

node 1 [ node "B" [], node "C" [] ]

Finally the type Interactive is used for programs interacting with the environment. We currently introduced only two forms of interaction, namely print and >>. Given a program p of type String, print p has type Interactive. This interactive program computes an interactive value which is meant to be triggered. Once the interactive value is triggered it prints the value of the text p on the screen.

The second form of interaction enables to sequence two interactive values. Given two programs p₁ and p₂ of type Interactive the program p₁ >> p₂ has type Interactive as well.

1.4 Program representation, meta-programming

When reading, writing, and editing programs we often work with the textual form of programs. We write programs in text files and so their representation is a sequence of characters in a file.

Machines do not directly accept this kind of program for execution. Even languages very close to the hardware such as assembly languages are not directly understood by the machine. Hence programs are processed by other programs. These programs processing other programs are called meta-programs and are described in greater detail in the following section.

Up to here our simple programming language can process numbers, text, lists, trees and interactive values. What about programs? What is required to process programs themselves? If a program is simply a text in a file then our text value can represent programs. Here are two programs, the second is the textual representation of the first:

2 * (10 + 11) { - this should compute 42 - }

"2 * (10 + 11) { - this should compute 42 - }"

This is common knowledge nowadays that the textual representation is not adapted for any non-trivial processing. A first step called lexing gets rid of the lexical issues of layout and comments. The lexing step turns
the program text to a list of words, called tokens. These tokens are often annotated by a token class to distinguish numbers, operators, constructs... Here is the same program as a simple list of tokens:

```
[ "2" , "*" , "(" , "10" , "+" , "11" , ")" ]
```

This representation is still unworkable for non-trivial processing. In particular there is too little structure in a list to reflect the program structure. To solve this issue, syntax trees have been introduced. Here is our same program, graphically depicted as a tree:

![Syntax Tree Diagram]

We picked names for some constructs such as “num” for numbers, “text” for text values, and “list” for lists. An exception is made for parentheses which no longer add any useful information and hence are not represented in the tree.

The process of translating text or tokens into a tree is called parsing. We will not discuss it more.

These syntax trees are generally called Abstract Syntax Trees or AST for short. Syntax trees are often said “abstract” because they no longer depend on some details of the “concrete” syntax.

Happily we have enough constructs in our language to build trees. We can hence show another representation of the same program as a tree built in our language:

```
node "*"
    [ node "num" [ node "2" [] ]
    , node "+"
        [ node "num" [ node "10" [] ]
        , node "num" [ node "11" [] ] ] ]
```

Representing programs of our language as values of our language itself is good to have but not necessary. However we can expect a programming language good at processing programs to be good at representing as many programs as possible.
How to choose the tree representation for a programming language? Here we made a simple choice: for each syntax rule we have a corresponding tree node labeled by the construct and with as many children as needed.

```hs
print "Hello! 2 times 21 is equal to " >>
print (show (2 * 21))
```

The syntax tree, graphically:

![Syntax Tree](image)

The syntax tree as a program:

```hs
node "" >>
  [ node "print"
    [ node "text"
      [ node "Hello! 2 times 21 is equal to " [] ]
    , node "print"
      [ node "show"
        [ node "*"
          [ node "num" [ node "2" [] ]
```

An example to illustrate lists:

```
[ "a", "b ++ c", show (2 + 3) ]
```

The syntax tree, graphically:

```
node "list"
  [ node "text" [ node "a" [] ]
    , node "++"
      [ node "text" [ node "b" [] ]
        , node "text" [ node "c" [] ] ]
    , node "show"
      [ node "+
          [ node "num" [ node "2" [] ]
            , node "num" [ node "3" [] ] ] ] ]
```
1.5. NAMES AND LOCAL BINDINGS

An example to illustrate trees:

node "A" [ node "B" [], node "C" [] ]

The syntax tree, graphically:

```
node
  text
    A
  list
    node
      text
        B
      list
    node
      text
        C
      list
```

The syntax tree as a program:

```
node "node"
  [ node "text" [ node "A" [] ]
    , node "list"
      [ node "node"
        [ node "text" [ node "B" [] ], node "list" [] ]
        , node "node"
          [ node "text" [ node "C" [] ]
            , node "list" [] ] ]
```

Meta-programming The broad topic of “programs processing other programs” is called meta-programming. Sometimes meta-programming is given narrower definitions, but we find this one to better account for the different parts of the research field. Meta-programming comprises the generation, analysis, transformation of programs or similar objects such as formulae and proofs. Some programming languages are completely designed around meta-programming to support run-time code generation (MetaML [Taha, 1999], ’C [Engler et al., 1996]). Program translations and optimizations, as done by compilers, are prime examples of meta-programming.

1.5 Names and local bindings

Our programming language, while capable of arithmetic computations, interactions, and program representation, lacks the concept of names. We
hence introduce a construct to give a name to part of a program and refer
to this part using the name. This enables an important goal of re-usability.
In a program we should avoid to repeat ourselves. Hence if two parts are the
same they may benefit from being written only once. Maybe more impor-
tantly, changes to this part of the software logic, during later evolution of
the code, only have to be done in one place instead of being duplicated. The
syntax of this new construct relies on three keywords \texttt{let}, \texttt{=} and \texttt{in}. If two
programs $p_1$ and $p_2$ are syntactically valid and $x$ is a name then
\texttt{let x = p_1 in p_2} is syntactically valid. Moreover, names (such as $x$) are valid program
themselves. If we want to print the same text twice we can write:

\begin{verbatim}
let x = print "Hello!" in x >> x
\end{verbatim}

If we replace the occurrences of $x$ by its definition (here \texttt{print "Hello!"})
we obtain a program with the same behavior:

\begin{verbatim}
print "Hello!" >> print "Hello!"
\end{verbatim}

The gain brought by sharing is significant. To illustrate this fact, we
build an artificial example where each added \texttt{let} would double the size of
the program if we could not use \texttt{let}. Albeit artificial this example conveys
the fact that sharing makes a big difference. The following example has 54
syntax nodes while the expanded version has 220 syntax nodes (only 124 if
we reduce $x_0$ to 0 first). Note also that the small computation done in $x_0$
can be performed only once instead of 16 times.

\begin{verbatim}
let x_0 = 42 ÷ 2 * 21 in
let x_1 = node x_0 [] in
let x_2 = node 1 [ x_1 , x_1 ] in
let x_3 = node 2 [ x_2 , x_2 ] in
let x_4 = node 3 [ x_3 , x_3 ] in
node 4 [ x_4 , x_4 ]
\end{verbatim}
1.6 Scoping

A crucial aspect of the `let` construct is the scope of the newly introduced name. Given a name `x` and two programs `p1` and `p2`, the program `let x = p1 in p2` defines `x` to be `p1` in `p2`. Thus, this makes `x` available in `p2`. We say that the scope of the name `x` is the program `p2`. We also say that `x` scopes over `p2`.

What should we do when a program uses a name that has not been defined? This is obviously an error and so should be detected as soon as possible. Here is an example to illustrate this kind of errors:

```
print x >>  -- x is not defined, hence this is an error
let x = x in -- x is not yet defined
print x     -- here x is defined
```

One may wonder if the same name could be used more than once. The scoping discipline we use allows this. In particular if one reuses a name already defined to define something else the new definition hides the previous one. Here is a correct program to illustrate the various scoping subtle cases:
let x = "1" in
print x >> -- this prints 1
let x = "2" in
print x >> -- this prints 2
print (let x = "3" in x) >> -- this prints 3
(let x = "4" in print x) >> -- this prints 4
print x >> -- this prints 2 again
let x = x ++ x in
print x >> -- this prints 22
let x = let x = "5" in x ++ x in
print x -- this prints 55

We now introduce some vocabulary about names. In the program \( \text{let } x = p_1 \text{ in } p_2 \), the name \( x \) is said to be \textit{bound}. In particular it is bound in \( p_2 \). We call the name \( x \) in this position a \textit{binder}. In the program \textit{print } x \textit{, the name } x \textit{ is said to be \textit{free}. We also call it an \textit{occurrence of } x \textit{.}

Sometimes names are also called \textit{variables}. We try to prefer the term \textit{name} over \textit{variable} in this document. More precisely we use the term \textit{variable} to represent the construct which holds just a name. For instance the program \( x + x \) contains two variables but only one name.

A program without any free names/variables is said to be closed. The set of free names can be defined inductively as follows. The set of free names of a variable \( x \) is the singleton set with the name \( x \). The free names of an operation such as \textit{print } p \textit{ or } \textit{show } p \textit{ are the free names of } p \textit{. The free names of an operation such as } \textit{p}_1 + \textit{p}_2 \textit{ are the union of free names of } \textit{p}_1 \textit{ and of } \textit{p}_2 \textit{. Finally the free names of } \textit{let } x = \textit{p}_1 \textit{ in } \textit{p}_2 \textit{ are the free names of } \textit{p}_2 \textit{ minus } x \textit{, union the free names of } \textit{p}_1.

A name \( x \) is said to be \textit{fresh} for a program \( p \) if the name \( x \) is not a member of the free variables of \( p \). For example the name \( y \) is fresh for the program \( \text{let } y = 42 \text{ in } x + y \), but the name \( x \) is not.

Two programs \( p_1 \) and \( p_2 \) are said to be \textit{\( \alpha \)-equivalent} if they differ only by a consistent renaming of the bound names. Note that this is not a formal description of \( \alpha \)-equivalence, but an informal definition appealing to our intuition of “name irrelevance”. Defining this relation precisely is one of the important part of this thesis. For instance the programs \( \text{let } x = 21 \text{ in } x + x \) and \( \text{let } y = 21 \text{ in } y + y \) are \( \alpha \)-equivalent. The name of a variable should not have any importance except being a tool to reference a position in the program without ambiguities. \( \alpha \)-equivalence is an equivalence relation. This means that the relation is reflexive (every program is \( \alpha \)-equivalent to itself), symmetric (if \( p_1 \) is \( \alpha \)-equivalent to \( p_2 \), then \( p_2 \) is \( \alpha \)-equivalent to \( p_1 \)), and transitive (if \( p_1 \) is \( \alpha \)-equivalent to \( p_2 \) and \( p_2 \) is \( \alpha \)-equivalent to \( p_3 \) then \( p_1 \) is \( \alpha \)-equivalent to \( p_3 \)). The \( \alpha \)-equivalence is also a congruence, meaning that if \( p_1 \) is \( \alpha \)-equivalent to \( p_2 \) then if we put the programs in the context \( C[\_] \) to produce bigger programs then \( C[ p_1 ] \) is \( \alpha \)-equivalent to \( C[ p_2 ] \).
Typing our `let` construct  We have introduced local definitions and variables and we now extend our typing discipline to these constructs. Like we have done for the previous constructs, we give the typing informally using a textual description. The program `let x = p_1 in p_2` has type $\sigma$ if and only if $p_1$ has some type $\tau$ and that $p_2$ has type $\sigma$ assuming that $x$ has type $\tau$. To type a variable we use the assumptions we gathered so far. There are several ways to precisely describe how to manage these assumptions, but we do not detail them in this introduction.

Let us try to check the typing with an example. We check that the program `let x = 42 in let y = show x in print y` has type `Interactive`. To do so we first check that `42` has type `N` which is true, then we must check that `let y = show x in print y` has type `Interactive` assuming that `x` has type `N`. To do so we first check that `show x` has type `String`, which given the rule for `show` amounts to check that `x` has type `N`, which is true by assumption. We then check that `print y` has type `Interactive` assuming that `y` has type `String`. Given the rule for `print` this amounts to check that `y` has type `String` which is true by assumption.

Meta-programming and representation of variables  How do we represent variables and the `let` construct? It is reasonable to start with names being values of type `String`, each variable being a tree node that we call `var`, and the `let` construct being a node with three subtrees. The program `let x = 6 in let y = x + 1 in x * y` can thus be depicted as:

![Diagram](image)

This first approach is the root of the `nominal` approach that we describe in greater detail in chapter 2.

A different approach is to use de Bruijn indices [de Bruijn, 1972]. This representation is said to be nameless because variables are no longer identified by a name but a notion of “distance” to the binding point. This nameless approach solves part of the problem by providing a canonical representation. However a major issue with this nameless representation is its
arithmetic flavor. Indeed properties about names and binders are turned into arithmetic formulae. This second approach is covered in chapter 5. Here is the same example using the de Bruijn style:

```
let
num 6
let
var 0
num 1
* var 1
* var 0
```

1.7 Empowering our language

**Declarations and definitions** We now fast-forward from our tiny subset of Agda to Agda itself as we need it in the remainder of this document. We start with declarations, which allow us to declare a symbol that can be used globally. This generally differs from the `let` construct whose scope is local. Moreover the declaration just specifies the type of the symbol. Subsequent phrases have to define this declared symbol. The declarations make use of the character `:` to separate the declared symbol from its type. The following line is read “Dear Agda, let us declare `hello-world` of type `Interactive`”:

```
hello-world : Interactive
```

After the declaration must come the definition. The name of the defined symbol is recalled and a program is given for its definition:

```
hello-world = print "Hello World!"
```

**Functions** We introduce a new sort of types, namely function types. If `σ` and `τ` are types then `σ → τ` is a type as well. This type represents functions whose domain is `σ` and co-domain is `τ`. Happily Agda functions are like mathematical functions and no surprise whatsoever will trouble this. The syntax for definitions enables the definitions of functions in a very simple way: we just give a name to the argument before the equal sign. To apply a
user defined function $f$ to an argument $x$, the syntax is the lightest syntax possible: $f \ x$.

```haskell
double : N → N
double n = n + n
```

```
-- This program prints: 42
prog1 : Interactive
prog1 = print (show (double 21))
```

The name $n$ before the equal sign is a binder and scopes over the sub-program found after the equal sign. The scoping works pretty much like with the \texttt{let} construct. Here is another example:

```haskell
hello : String → Interactive
hello s = print ("Hello " ++ s ++ "!")
```

```
-- This program prints: Hello Functional World!
prog2 : Interactive
prog2 = hello "Functional World"
```

In order to receive multiple arguments one simply has to make functions return functions. Indeed the type $N \to (N \to N)$ is the type of a function taking a first number argument and returning a function taking a second number argument to finally deliver its result number. This is a pattern so common that we make the arrow type associate on right such that we can write the type this way: $N \to N \to N$. The same shortcut goes for function applications. Instead of writing $(f \ x) \ y$ or worse $(f(x))(y)$ we simply make the application associate on left, thus we can write $f \ x \ y$.

Here is an example:

```haskell
hello2 : String → N → Interactive
hello2 s n = print ("Hello " ++ s ++ " " ++ show n ++ "!")
```

```
-- This program prints: Hello World 42!
prog3 : Interactive
prog3 = hello2 "World" (2 * 21)
```

\textbf{Data-types} Among the types presented so far, $N$, \texttt{List}, \texttt{Tree} are user-defined in AGDA. The general mechanism used to define these types is called \textit{inductive families}. Inductive families generalize various forms of definition mechanisms such as \textit{sum and product types}, \textit{regular tree types}, \textit{algebraic
data types, and GADTs (generalized algebraic data-types). To define an
inductive family, we need to declare its name and type, and declare as many
data constructors as we want. Each data constructor has a name and a type
as well. Let us study the definition for \texttt{Bool}, one of the simplest data type
possible:

```agda
data Bool : Set where
  false : Bool
  true : Bool
```

The first line declares \texttt{Bool} to have type \texttt{Set}. Indeed \texttt{Set} is a special
type which is the type of basic types. Agda treats types like other values of
the language. Then we define two data constructors called \texttt{false} and \texttt{true}.
These two constructors are the two only values of type \texttt{Bool}.

We now focus on the type of natural numbers, namely \texttt{N}:

```agda
data N : Set where
  zero : N
  suc : N \to N
```

The first line declares \texttt{N} to have type \texttt{Set}. Then we define two data
constructors called \texttt{zero} and \texttt{suc}. The constructor \texttt{zero} is introduced as
a value of type \texttt{N} to represent the number 0. The constructor \texttt{suc} (for
successor) is introduced as a function from \texttt{N} to \texttt{N} which might seem like a
surprising beast. Two points are striking. First we are using the type \texttt{N} in
its own definition: this type is said to be recursive. The second point is to
declare a function without giving it a definition. Indeed \texttt{suc} has no other
definition, and thus giving it an argument does not trigger a computation.
For instance \texttt{suc zero} stays stuck like that and does not reduce further. The
language is built to take advantage of data constructors to define functions
by pattern matching.

Note that the same name can be used for different data constructors
of distinct data types. Agda makes use of type annotations to resolve
ambiguities.

To illustrate definitions made with pattern matching the following pro-
gram defines a function called \texttt{not} which negates a Boolean value:

```agda
not : Bool \to Bool
not true = false
not false = true
```

This definition is made of two equations: one for each constructor of the
inspected argument. In the case for \texttt{true} we return \texttt{false} and in the case
for \texttt{false} we return \texttt{true}.
1.7. EMPOWERING OUR LANGUAGE

We now go on a more interesting definition made with pattern matching. The following program defines a function called triple which multiplies its argument by three:

\[
\text{triple} : \mathbb{N} \rightarrow \mathbb{N}
\]

\[
\begin{align*}
\text{triple zero} &= \text{zero} \\
\text{triple} (1 + n) &= 3 + 3 \times n \\
\text{triple} (\text{suc} n) &= \text{suc} (\text{suc} (\text{suc} (\text{triple} n)))
\end{align*}
\]

While this definition is longer than we could expect (\text{triple} n = 3 \times n), it has a pedagogical interest. This definition is made of two equations: one for each constructor of the inspected argument. In the successor case the function triple is used in the definition of triple itself! This function is said to be recursive.

We can now reveal that all the operations on natural numbers we have seen so far are actually defined within the language using recursive definitions. Here are for instance the definitions for + and \times. To express that we want these operators to be infix, we declare + as _+_ and \times as _*_.

\[
\begin{align*}
\_+_ : \mathbb{N} \rightarrow \mathbb{N} \rightarrow \mathbb{N} \\
\text{zero} + n &= n & \text{-- 0} + n &= n \\
\text{suc} m + n &= \text{suc} (m + n) & \text{-- (1} + m) + n &= 1 + (m + n)
\end{align*}
\]

\[
\begin{align*}
\_*_ : \mathbb{N} \rightarrow \mathbb{N} \rightarrow \mathbb{N} \\
\text{zero} \times n &= \text{zero} & \text{-- 0} \times n &= 0 \\
\text{suc} m \times n &= m + m \times n & \text{-- (1} + m) \times n &= n + m \times n
\end{align*}
\]

The notation we used for literal numbers such as 2 or 4 is actually strictly equivalent to \text{suc (suc zero)} and \text{suc (suc (suc (suc zero)))} respectively.

We define a last operation on natural numbers, namely division by two. We do not show the definition for \div. Indeed, division by a known constant is indeed much simpler to define recursively and illustrates subtler pattern matching. The function is declared as _/2 and hence has to be used either prefix as _/2 4 or postfix as 4 _/2. You can notice how spaces are of prime importance in Agda since they allow to freely choose meaningful names for functions. The function _/2 proceeds as follows. The two base cases for zero and one are handled in the first two equations. The last equation deals with all numbers strictly greater than one which makes a simple recursive call to
obtain our result:

\[-/2 : \mathbb{N} \rightarrow \mathbb{N}\]

\[- 0 / 2 = 0\]

\[- \text{zero} / 2 = \text{zero}\]

\[- 1 / 2 = 0\]

\[- \text{suc zero} / 2 = \text{zero}\]

\[- (2 + n) / 2 = 1 + n / 2\]

\[- \text{suc (suc n)} / 2 = \text{suc (n / 2)}\]

**Polymorphism**  Sometimes functions do not need to know the nature of parts of their arguments. This means that many types could be acceptable for such functions. An extreme case is the identity function which simply returns its argument. What type should we give it? \( \mathbb{N} \rightarrow \mathbb{N} \), \( \text{String} \rightarrow \text{String} \), or \( \text{List} \mathbb{N} \rightarrow \text{List} \mathbb{N} \) and the list goes on indefinitely. The solution to this issue is called *polymorphism*. We generalize the type of the function type to \( \forall \{\text{A}\} \rightarrow \text{A} \rightarrow \text{A} \), which reads “for all type \( \text{A} \) a function from \( \text{A} \) to \( \text{A} \)”. The polymorphic identity function \( \text{id} \) can thus be written:

\[\text{id} : \forall \{\text{A}\} \rightarrow \text{A} \rightarrow \text{A}\]

\[\text{id} \ x = x\]

\[- \text{The function id can be used at different types}\]

\[\text{prog}_4 : \text{Interactive}\]

\[\text{prog}_4 = \text{print} (\text{id} \ "Hello " ++ \text{show} (\text{id} \ 42))\]

**Lists**  We define two new data types that we assumed to be special so far, namely **List** and **Tree**. The type for lists –such as the type \( \mathbb{N} \)– is made of two data constructors. A base constructor named \([\] \) and pronounced “nil” represents the empty list. Another constructor named \( \_::\_ \) and pronounced “cons” appends one element to the front of a list. The notation \([ n_1 \ , \ n_2 \ , \ ... \ ] \) is simply a shorthand for the less familiar \( n_1 :: n_2 \ ... :: [] \).

\[
\text{data List} \ (\text{A} : \text{Set}) : \text{Set} \ \text{where} \\
\text{[]} : \text{List} \ \text{A} \\
\_::\_ : \text{A} \rightarrow \text{List} \ \text{A} \rightarrow \text{List} \ \text{A}
\]

Plenty of interesting functions can be defined recursively on lists. We
show one of them which while being simple can be insightful. The function \texttt{length} takes a list and returns its length as a natural number. The function is defined with two equations: one for the empty list whose length is zero, and one for any constructed list whose length is the successor of the length of the \textit{tail} of the list. In short this function replaces the lists constructors by the constructors of natural numbers. This highlights the fact that both types share the same structures. Natural numbers are lists of meaningless elements and lists are natural numbers whose constructors are annotated by elements. The function \texttt{length} is polymorphic. It takes a list, forgets the elements to reveal the bare structure behind any list: a natural number.

\begin{verbatim}
length : ∀{A} → List A → N
length [] = zero
length (x :: xs) = suc (length xs)
\end{verbatim}

Let us remark that since we make no use of the name \texttt{x} in the second equation for \texttt{length} we could have use the special \texttt{wildcard} pattern. The wildcard pattern is noted \_ and is used to replace a name to state that we do not use this part of the value.

Another common function on lists is the function \texttt{map}. The function \texttt{map} takes a function \texttt{f} from a type \texttt{A} to a type \texttt{B}, and also takes a list of type \texttt{List A} on which it applies \texttt{f} on every element to build the resulting list of type \texttt{List B}. Since \texttt{map} takes a function as argument it is what we call an \textit{higher-order} function. Moreover, the function \texttt{map} is also recursive and polymorphic. Here is the definition of \texttt{map}:

\begin{verbatim}
map : {A B : Set} → (A → B) → List A → List B
map f [] = []
map f (x :: xs) = f x :: map f xs
\end{verbatim}

We now introduce an extension to pattern matching equations, namely the \texttt{with} construct. This construct extends a pattern-matching-based definition with new columns. This construct is of great effect when combined with dependent pattern-matching. However, we present it here on a simpler example, the function to filter a lists. The function \texttt{filter}, takes a predicate \texttt{p} and a list \texttt{xs} and keeps only the elements of \texttt{xs} which satisfy the predicate \texttt{p}. The \texttt{with} construct is used here to select a branch according to the result of the predicate:
filter : {A : Set} → (A → Bool) → List A → List A
filter p [] = []
filter p (x :: xs) with p x
filter p (x :: xs) | true = x :: filter p xs
filter p (x :: xs) | false = filter p xs

Moreover, an ellipsis . . . can be used to elide a redundant equation prefix. Hence we can write filter, this way:

filter : {A : Set} → (A → Bool) → List A → List A
filter p [] = []
filter p (x :: xs) with p x
... | true = x :: filter p xs
... | false = filter p xs

Trees and forests We continue with trees the exploration of our previously assumed basic types. Trees can be defined with a new data type. This data type Tree has a single data constructor named node with two arguments: the node label of type A and the children as a list of subtrees (List (Tree A)).

data Tree (A : Set) : Set where
  node : A → List (Tree A) → Tree A

Commonly we call forests the lists of trees. The name is suggestive and the type is shorter to write. Its definition shows how types are treated such as other values:

Forest : Set → Set
Forest A = List (Tree A)

Trees and forests are interdependent. They finally build a pair of mutually recursive types. This is the occasion to define a pair of mutually recursive functions. We define sumTree and sumForest which respectively compute the sum of the labels in a tree of natural numbers and in a forest of natural numbers. For AGDA to accept these definitions, the two declarations must come before the two definitions.

sumTree : Tree N → N
sumForest : Forest N → N

\[
\text{sumTree} \ (\text{node n forest}) = n + \text{sumForest forest} \\
\text{sumForest} \ [] = 0 \\
\text{sumForest} \ (\text{tree :: forest}) = \text{sumTree tree} + \text{sumForest forest}
\]

Robust program representations  So far we have seen three distinct types to represent programs: text values (String), lists of tokens (List String), and trees (Tree String). These three types are based on the type String and thus they are loose representations. For instance the tokens can be malformed tokens and the tree labels could be malformed as well. We could introduce data types for tokens and tree labels which rule out the malformed text values. However we can do even better. Here is a data type for our tiny programming language of the beginning:

```haskell
data Program : Set where  
  'num : N → Program  
  'text : String → Program  
  'list : List Program → Program  
  'node : Program → Program → Program  
  '+' : Program → Program → Program  
  '-' : Program → Program → Program  
  '*' : Program → Program → Program  
  '/' : Program → Program → Program  
  '++ : Program → Program → Program  
  'print : Program → Program  
  'show : Program → Program  
  '>> : Program → Program → Program  
  'var : String → Program  
  'let : String → Program → Program → Program
```

The type Program is a recursive type inducing a specialized tree structure. Each construct is modeled by a single data constructor which is named with the corresponding label we have for trees plus an extra ‘ character. The data constructor also specifies how many subtrees are expected and what kind of subtree is expected. Here are two of our previous examples represented with our type Program:

```haskell
prog4 : Program
prog4 = '*' ('num 2) ('+ ('num 10) ('num 11))
```
Here are now a few programs that cannot be represented with the data type Program. Indeed while all correct programs can be represented, this simple data type already rules out plenty of wrong programs. Here is first a list of syntactically wrong programs represented as texts:

```
[ "2 *" -- missing operand
, "(2" -- missing parenthesis
, "2 {- " -- non-closed comment
, "bla" -- unknown construct or variable
]
```

Here is now a list of still syntactically wrong programs represented as trees:

```
[ node "+" [ p ] -- missing operand
, node "+" [ p₁, p₂, p₃ ] -- extra operand
, node "bla" [] -- unknown construct
, node "var" [ node "bla" [] ] -- unknown variable
]
```

Finally, there are still wrong programs accepted by all of our representations. Those are the ill-scoped programs and the ill-typed programs. Here is a list of ill-scoped or ill-typed programs using the type Program:

```
[ 'var "bla" -- unknown variable
, '+ (\text{num 1}) (\text{Hello!}) -- ill-typed
, 'let "x" (\text{var "x"}) (\text{num 1}) -- unknown variable
]
```

The rest of this document focuses on how to improve program representation to better account for the handling of variables in programs.

**Declaring the last operations** We have shown how various constructs of our tiny programming language can be defined in Agda. We now quickly declare the remaining constructs that can be Agda functions. Thus we declare `-`, `\div`, `show`, `++`, `print`, and `>>>`. While we give no definitions for these functions the declarations describe both their syntax and their
1.7. EMPOWERING OUR LANGUAGE

typing very concisely:

\[-\_\_\_ : \mathbb{N} \to \mathbb{N} \to \mathbb{N}\]
\[-\_\_\_ : \mathbb{N} \to \mathbb{N} \to \mathbb{N}\]
\[\text{show} : \mathbb{N} \to \text{String}\]
\[\_\_\_\_ : \text{String} \to \text{String} \to \text{String}\]
\[\text{print} : \text{String} \to \text{Interactive}\]
\[\_\_\_\_ : \text{Interactive} \to \text{Interactive} \to \text{Interactive}\]

The core constructs from our tiny language that we do not define are literals (numbers, texts, lists), variables and the \texttt{let} construct. However, in order to use all these functions and constructors we introduced a fairly-discrete construct, namely application. Since application is written as a simple juxtaposition (using spaces or parentheses) we might forget it. In our tree representation we use the label "\texttt{app}" for these application nodes. We can now view the example program $2 \times (10 + 11)$ as a tree where the application nodes replace the special nodes of operations:

\[\begin{array}{c}
\text{app} \\
\text{app} \\
\_\_\_\_ \quad \text{num} \\
\_\_\_\_ \quad \text{app} \\
\text{num} \\
2 \quad \_\_\_ \quad \text{num} \\
10 \\
\_\_\_\_ \quad \text{num} \\
11 \\
\end{array}\]

\textbf{Agda types} In \texttt{Agda}, the usual function space is written $A \to B$, while the dependent function space is written $(x : A) \to B$ or $\forall (x : A) \to B$. An implicit parameter, introduced via $\forall\{x : A\} \to B$, can be omitted at a call site if its value can be inferred from the context. There are shortcuts for introducing multiple arguments at once or for omitting a type annotation, as in $\forall\{A\} \{i,j : A\} \to e$.

In \texttt{Agda}, \texttt{Set} (or \texttt{Set}_0) is the type of small types such as $\mathbb{N}$, \texttt{List} \texttt{String}, and \texttt{Maybe} $(\mathbb{B} \times \mathbb{N})$. \texttt{Set}_1 is the type of $\texttt{Set}, \texttt{Set} \to \texttt{ Bool}, \mathbb{N} \to \texttt{Set}$, and $\texttt{Set} \to \texttt{Set}$.

There is no specific sort for propositions in \texttt{Agda}: everything is in $\texttt{Set } \ell$ for some $\ell$. The unit type is a record type with no fields named $\top$. It also represents the \texttt{True} proposition. The empty type is named $\bot$ and is an
(inductive) data type with no constructors. It also represents the \textbf{False} proposition. The negation \( \neg A \) is defined as \( A \rightarrow \bot \).

**Lexical conventions** We recall that \textsc{Agda} is strict about whitespace: \( x \leq y \) is an identifier, whereas \( x \leq y \) is an application. This allows naming a variable after its type (deprived of any whitespace). For example, \( x \leq y \) might be a variable of type \( x \leq y \), that is, a proof of \( x \leq y \).

**Various notions of equality** Advanced logics and proof systems exhibit various forms of equality. The \textit{definitional equality} is a first form of equality which is deeply rooted in the computation rules of the programming language itself, here, \textsc{Agda}. Two terms are \textit{definitionally equal} if and only if they can both reduce to a common term. In \textsc{Agda}, the reduction is a combination of \( \beta \)-reductions, \( \eta \)-conversions, and application of the definition equations.

Here are a few examples of definitionally equal terms. We informally use \( = \) for this equality since this symbol is the one used for definitions.

\[
(\lambda x \rightarrow x) \text{ suc zero} = \text{ suc zero} \\
\text{ suc} = \lambda x \rightarrow \text{ suc} x \\
\text{ zero} + n = n
\]

Here is an example of two terms which are not definitionally equal even if this equality seems natural:

\( n + \text{ zero} \neq n \)

Definitional equality is completely automatic and thus requires no help from the user. However if we want to include some reasoning steps we can use the \textit{propositional equality}. The symbol used in \textsc{Agda} and further in this document is \( \equiv \). To simplify matters, here is the definition of the propositional equality specialized to values of small types (\( \text{Set}_0 \)), namely \( \equiv_0 \):

\[
\text{data} \ _\equiv_0 \{ A : \text{Set}_0 \} \ (x : A) : A \rightarrow \text{Set}_0 \ \text{where} \\
\text{ refl : } x \equiv_0 x \\
\text{ x }\not\equiv_0 y = \neg(x \equiv_0 y)
\]

We do not intend to explain the subtleties of such a definition. We only mention that there is a single constructor for this type requiring both sides to be same, hence definitionally equal.
EMPOWERING OUR LANGUAGE

-- This is definitionally true, hence immediately proven by refl
  zero + n \equiv n

-- This is provable by a simple induction on n
  \forall n \rightarrow n + zero \equiv n

Sometimes, two functions \( f \) and \( g \) cannot be proved propositionally equal but still produce the same output on every possible input. In this case, the functions \( f \) and \( g \) are said to be \textit{equal pointwise}. The symbol for pointwise equality is \( \simeq \). Here is the definition of pointwise equality in AGDA, specialized to small types (\( \text{Set}_0 \)), non-dependent functions:

\[
\simeq_{\text{pointwise}}^0 \colon \{A B : \text{Set}_0\} (f g : A \rightarrow B) \rightarrow \text{Set}_0
\]
\[
f \simeq_{\text{pointwise}}^0 g = \forall x \rightarrow f x \equiv_0 g x
\]

To illustrate pointwise equality we define the function \( \text{not}^2 \) which iterates the function \( \text{not} \) two times.

\[
\text{not}^2 : \text{Bool} \rightarrow \text{Bool}
\]
\[
\text{not}^2 x = \text{not} (\text{not } x)
\]

We then show that the function \( \text{not}^2 \) is equal pointwise to the identity function. Given the definitions for \( \simeq_{\text{pointwise}}^0 \) and \( \text{not}^2 \) this exactly amounts to show: \( \forall x \rightarrow \text{not} (\text{not } x) \equiv x \).

\[
\text{not}^2 \simeq_{\text{pointwise}}^0 \text{id}
\]
\[
\text{not}^2 \text{id} \text{ true } = \text{refl} -- \text{true } = \text{not} (\text{not } \text{true}) \text{ definitionally}
\]
\[
\text{not}^2 \text{id} \text{ false } = \text{refl} -- \text{false } = \text{not} (\text{not } \text{false}) \text{ definitionally}
\]

Equalities are said to be either intensional or extensional. Let us use sorting functions as an example to illustrate the difference. If we have two different sorting functions each implementing one sorting algorithm such as bubble sort and quick sort. The two functions are said to be extensionally equal since they both return the same sorted list for any given list. However bubble sort and quick sort are not intentionally equal. The \textit{intention} is actually opposite. When we write a quick sort function, we intentionally want to make it different than bubble sort!

In AGDA both the definitional and the propositional equalities are currently intensional. There is an ongoing will to make the propositional equality more extensional. While this sounds like a radical change, the propositional equality is actually already compatible with extensionality. Indeed, there is no way to contradict extensionality with the current propositional equality. In short there is no proof than quick sort is different from bubble sort and thus making them provably equal introduce no contradiction.
The pointwise equality is by construction extensional and in section 4.2 we explain a generalized definition to relate functions which sends related inputs to related outputs.

**Full development online** We use some definitions from Agda’s standard library: natural numbers, booleans, lists, and applicative functors (pure and \_\_\_\_\_). For the sake of conciseness, the code fragments presented in this document are sometimes not perfectly self-contained. However, a complete Agda development is available online [Pouillard, 2011a].

**Outline** This document is organized as follows. The next three chapters delve into the nominal approach. We introduce the nominal approach (chapter 2) and present our system: a safe programming interface for the nominal style. We then present how to use it (chapter 3), and what happens behind the scene to implement it and show its safety (chapter 4).

The next chapter (5) covers a nameless approach known as “de Bruijn indices”. We present how to seamlessly extend our system to this new approach. This chapter covers the same aspects: the interface and its implementation, its usage, its soundness.

The remaining chapter (6) discusses different variations and combinations of these variations. At the same time this chapter covers the related work and concludes.
Chapter 2

The nominal approach

This chapter is organized as follows. The first section informally introduces and presents several techniques to represent data structures with bindings in a nominal style. Section 2.2 describes our solution, an interface to program with names and binders.

2.1 Introduction to the nominal approach

2.1.1 Warm-up: the bare nominal approach

The bare approach to abstract syntax with names and binders in nominal style requires very little infrastructure to start with. Names and binders are represented by so-called atoms. The set of atoms is countably infinite and the only required operation is an equality test. Using natural numbers as a concrete representation for atoms is a common and sensible choice.

-- A set of atoms (could be N)
Atom : Set

-- Atom is countably infinite; here are some atoms:
-- x,y,z... could be represented by 0,1,2...
x y z f g {-.--} : Atom

-- The equality test on atoms
==^A_ : (x y : Atom) → Bool

Given the type Atom we can readily define algebraic data types for abstract syntax with names and binders. Our running example is the untyped λ-calculus defined below. The type Tm^A (Tm for “term” and ^A for “atom”) is made of three data constructors. The constructor V is for variables and simply holds an atom. The constructor _ is the function application construct made of two subterms. The constructor x takes an atom and a subterm
in which this atom is considered bound. This means that the construct $\times$ is introducing a variable. On contrary the atom in the construct $\forall$ is said to be free. Indeed this atom is supposed to refer to a bound atom. The constructor Let also takes an atom but two subterms. The atom is bound in the second subterm only.

\[
data 
  \text{Tm}^A : \text{Set} \, \text{where} \\
  V : (x : \text{Atom}) \to \text{Tm}^A \\
  \_ \_ \_ : (t \, u : \text{Tm}^A) \to \text{Tm}^A \\
  \times : (b : \text{Atom}) (t : \text{Tm}^A) \to \text{Tm}^A \\
  \text{Let} : (b : \text{Atom}) (t \, u : \text{Tm}^A) \to \text{Tm}^A
\]

It is striking that there is no formal distinction between the atoms that represent binders and those that represent occurrences. Neither is there any indication of the scope of the binders. This calls for improvement.

We consider it very important to highlight that atoms are used for two distinct purposes whether they are in a binding position or a free position. Starting from section 2.2, we embrace that distinction and provide distinct types for these usages.

Here are two term examples, the identity function and the application function:

\[
\begin{align*}
-- \, \lambda x. \, x \\
idTm^A : \text{Tm}^A \\
idTm^A &= \times x (\forall x)
\end{align*}
\]

\[
\begin{align*}
-- \, \lambda f. \, \lambda x. \, f \, x \\
apTm^A : \text{Tm}^A \\
apTm^A &= \times f (\times x (\forall f \cdot \forall x))
\end{align*}
\]

The strength of this approach resides in its simplicity. The representation of terms closely follows the concrete syntax of the language. The main issue is adequacy: there are multiple equivalent representations of the “same” term.

Indeed the choice of atoms is fairly arbitrary. Two terms can represent the same piece of syntax when they differ only by a consistent renaming of bound names. In this situation two such terms are said to be $\alpha$-equivalent. Here are for example two $\alpha$-equivalent terms:

\[
\begin{align*}
t^x & : \text{Tm}^A \\
t^x &= \times x (\forall f \cdot \forall x) \\
t^y & : \text{Tm}^A \\
t^y &= \times y (\forall f \cdot \forall y)
\end{align*}
\]
2.1. INTRODUCTION TO THE NOMINAL APPROACH

The term $t^x$ is $\alpha$-equivalent to $t^y$ since consistently renaming the bound name $x$ by $y$ in the term $t^x$ yields the term $t^y$. Respectively consistently renaming $y$ by $x$ in $t^y$ yields $t^x$. However $\alpha$-equivalence can be subtle, let us observe a third term $t^f$ which is not $\alpha$-equivalent to neither $t^x$ nor $t^y$:

$$t^f : \mathbf{Tm}^A$$
$$t^f = \forall f (V f \cdot V f)$$

An inconsistent renaming of the bound name $x$ by $f$ in $t^x$ yields $t^f$, while a consistent renaming of the bound name $f$ by $x$ in $t^f$ does not yield $t^x$.

We do not delve more into the details of $\alpha$-equivalence yet. We focus on the fact that the concrete naming of a term is a representation issue and should not be relevant for the computation. In particular, good functions should be independent of this representation issue. This property can be stated as follows:

A function is well-behaved if, when applied to $\alpha$-equivalent arguments, it produces $\alpha$-equivalent results.

To illustrate well-behaved functions we give a few examples. The following functions $\mathbf{rm}^A$ (removes an atom from a list) and $\mathbf{fv}$ (lists the free variables/atoms of a term) are well-behaved:

$$\mathbf{rm}^A : \mathbf{Atom} \rightarrow \mathbf{List} \mathbf{Atom} \rightarrow \mathbf{List} \mathbf{Atom}$$
$$\mathbf{rm}^A _- [] = []$$
$$\mathbf{rm}^A x (y :: ys) =$$
   if $x ==^A y$ then $\mathbf{rm}^A x ys$
   else $y :: \mathbf{rm}^A x ys$

   -- Since $\mathbf{rm}^A$ behaves well, this holds:
   test-$\mathbf{rm}^A : \mathbf{rm}^A x [ x ] \equiv \mathbf{rm}^A y [ y ]$
   test-$\mathbf{rm}^A = \mathbf{refl}$ -- both reduces to $[]$

$$\mathbf{fv} : \mathbf{Tm}^A \rightarrow \mathbf{List} \mathbf{Atom}$$
$$\mathbf{fv} (V x) = [ x ]$$
$$\mathbf{fv} (t \cdot u) = \mathbf{fv} t ++ \mathbf{fv} u$$
$$\mathbf{fv} (\forall x t) = \mathbf{rm}^A x (\mathbf{fv} t)$$
$$\mathbf{fv} (\mathbf{Let} x t u) = \mathbf{fv} t ++ \mathbf{rm}^A x (\mathbf{fv} u)$$

   -- Since $\mathbf{fv}$ behaves well, this holds:
   test-$\mathbf{fv} : \mathbf{fv} t^x \equiv \mathbf{fv} t^y$
   test-$\mathbf{fv} = \mathbf{refl}$ -- both reduces to $[ f ]$
We now illustrate misbehaving functions with two examples. The function \( \text{ba} \) computes the list of bound atoms. The function \( \text{cmp-ba} \) takes two terms and compare their bound variables if both are \( \alpha \) constructs.

\[
\begin{align*}
\text{ba} : Tm^A &\rightarrow \text{List Atom} \\
\text{ba} (\forall x \ t) &= x :: \text{ba} \ t \\
\text{ba} (\text{Let} \ x \ t \ u) &= x :: \text{ba} \ t :: \text{ba} \ u \\
\text{ba} (t \cdot \ u) &= \text{ba} \ t ++ \text{ba} \ u \\
\text{ba} (V \ _) &= [] \\
\end{align*}
\]

\([x] \neq [y] : [ x ] \neq [ y ] \\
[x] \neq [y] = \{ ! \text{ omitted } ! \}
\]

\[
\begin{align*}
\text{-- Since ba does not behave well:} \\
\text{test-ba} : \text{ba} \ t^x \neq \text{ba} \ t^y \\
\text{test-ba} &= [x] \neq [y] \\
\text{cmp-ba} : Tm^A &\rightarrow Tm^A \rightarrow \text{Bool} \\
\text{cmp-ba} (\forall x \ _) (\forall y \ _) &= x ==^A y \\
\text{cmp-ba} (\_) (\_) &= \text{false} \\
\end{align*}
\]

\[
\begin{align*}
\text{-- Since cmp-ba does not behave well:} \\
\text{test-cmp-ba} : \text{cmp-ba} \ t^x \neq \text{cmp-ba} \ t^y \\
\text{test-cmp-ba} (\_) -- \text{true} \neq \text{false} \\
\end{align*}
\]

In traditional informal developments, \( \alpha \)-equivalence is identified with equality. The upside is that every definition respects \( \alpha \)-equivalence. Hence functions automatically map \( \alpha \)-equivalent inputs to \( \alpha \)-equivalent outputs. The downside is that building functions is more difficult. Indeed what were misbehaving functions before, are not functions anymore when we identify \( \alpha \)-equivalence and equality. They are not functions simply because they map equal inputs to different outputs.

One of the goals of our system is to guarantee that well-typed functions are well-behaved. A function like \( \text{cmp-ba} \) is ill-typed in our system. A function like \( \text{ba} \) is typed differently than the function \( \text{fv} \), effectively disarming the function \( \text{ba} \).

### 2.1.2 Using well-formedness judgements

One way to define the scoping rules is to define a well-formedness judgement. It can be done using a recursive predicate over the structure of terms. It is a well-known technique used in the definition of type systems. The standard presentation makes use of a set of inference rules where judgements are
made of an environment, a term and a type. The environment tracks the
type of each introduced variable. To specify scoping rules one follows the
same presentation but without the types. We directly focus on a formal
presentation in Agda since inference rules (and grammars) have a direct
translation into inductive types. First one defines the environments which
are nothing more than lists of atoms:

```agda
data Env : Set where
  ϵ  : Env
  _₋₋ : (Γ : Env) (x : Atom) → Env
```

Then comes the definition of the membership predicate. It states when
an atom is a member of some environment. This is done through two rules:
one applies when the atom is present at the first position of the environment,
and a second rule applies when is present in the tail of the environment. Here
is the definition in Agda where lines drawn with comments give constructors
a flavor of inference rules (a comment starts with -- and stops at the end
of line):

```agda
data _∈_ x : (Γ : Env) → Set where
  here : ∀ {Γ} → ------------------
         x ∈ (Γ , x)

  there : ∀ {Γ y} → x ∈ Γ
           → ------------------
           x ∈ (Γ , y)
```

Finally one can state the scoping rules for the λ-calculus. The definition
boils down to using an environment to track bound atoms, using the mem-
bership predicate at variable occurrences and pushing the binders onto the
environment:
data \vdash \Gamma : \text{Tm}^A \rightarrow \text{Set} \quad \text{where}
\begin{align*}
V : \forall \{x\} &\quad \rightarrow x \in \Gamma \\
&\quad \rightarrow \quad \Gamma \vdash V x \\
\_ \_ \_ : \forall \{t \ u\} &\quad \rightarrow \Gamma \vdash t \\
&\quad \rightarrow \Gamma \vdash u \\
&\quad \rightarrow \quad \Gamma \vdash t \cdot u \\
\chi : \forall \{t \ b\} &\quad \rightarrow \Gamma , \ b \vdash t \\
&\quad \rightarrow \quad \Gamma \vdash \chi \ b \ t \\
\text{Let} : \forall \{t \ u \ b\} &\quad \rightarrow \Gamma \vdash t \\
&\quad \rightarrow \Gamma , \ b \vdash u \\
&\quad \rightarrow \quad \Gamma \vdash \text{Let} \ b \ t \ u
\end{align*}

We can now state that our example terms are well-scoped in the empty environment. Thanks to implicit arguments and to the definition of the membership predicate, the proof that a term is well-scoped is the term itself in de Bruijn notation (\text{zero} is \text{here} and \text{suc} is \text{there}).

\[\vdash \text{id} : \epsilon \vdash \text{idTm}^A\]
\[\vdash \text{id} = \chi (V \ \text{here})\]

\[\vdash \text{ap} : \epsilon \vdash \text{apTm}^A\]
\[\vdash \text{ap} = \chi (\chi (V (\text{there here}) \cdot V \ \text{here}))\]

The use of \text{Agda} implicit arguments keep these examples concise. The curious reader who is unfamiliar with \text{Agda} might find interesting to look at the same (second) example with all arguments made explicit:

\[\vdash \text{ap}' : \epsilon \vdash \text{apTm}^A\]
\[\vdash \text{ap}' = \chi \{\epsilon\} \{\chi \ x \ (V \ f \cdot V \ x)\} \{f\}\]
\[\chi \{\epsilon, f\}\{V \ f \cdot V \ x\} \{x\}\]
\[\{V \{\epsilon, f, x\} \{f\}\}
\[\{\text{there} \{f\} \{\epsilon, f\} \{x\}\}
\[\{\text{here} \{f\} \{\epsilon\}\}\} \cdot
\[V \{\epsilon, f, x\} \{x\}\]
\[\{\text{here} \{x\} \{\epsilon, f\}\}\})\]

However this technique is not directly what we are looking for. Indeed
these scoping properties are explicitly stated on the side of each definition. We are looking for something more integrated into the types. This would enable well-formedness to be enforced in a more pervasive and automatic manner. Happily this technique can be adapted to merge the scoping information and the term.

2.1.3 Well-scoped terms

Merging terms and scoping rules is not a new technique and amounts to removing the term index of the scoping predicate. The resulting term type is indexed by an environment. This environment is extended at binders and queried at variable occurrences:

\[
data Tm^J \Gamma : \text{Set where} \begin{align*}
\forall \{ x \} & \to x \in \Gamma \to Tm^J \Gamma \\
\cdot \cdot & : Tm^J \Gamma \to Tm^J \Gamma \to Tm^J \Gamma \\
\chi & : \forall b \to Tm^J (\Gamma, b) \to Tm^J \Gamma \\
\text{Let} & : \forall b \to Tm^J \Gamma \to Tm^J (\Gamma, b) \to Tm^J \Gamma
\end{align*}
\]

One can define our two term examples in this style as well:

\[
\begin{align*}
idTm^J & : Tm^J \epsilon \\
idTm^J & = \chi x (V \text{ here}) \\
apTm^J & : Tm^J \epsilon \\
apTm^J & = \chi f (\chi x (V \text{ (there here)} \cdot V \text{ here}))
\end{align*}
\]

The function \(fv\) can easily be adapted to this style, while the function \(rm^A\) can be reused:

\[
\begin{align*}
fv : \forall \{ \Gamma \} & \to Tm^J \Gamma \to \text{List Atom} \\
fv (V \{x\} \cdot) & = [x] \\
fv (t \cdot u) & = fv t ++ fv u \\
fv (\chi x t) & = rm^A x (fv t) \\
fv (\text{Let} x t u) & = fv t ++ rm^A x (fv u)
\end{align*}
\]

Alas the functions \(ba\) and \(cmp-ba\) are not rejected by this style. Their types becomes:

\[
\begin{align*}
ba : \forall \{ \Gamma \} & \to Tm^J \Gamma \to \text{List Atom} \\
cmp-ba : \forall \{ \Gamma_1, \Gamma_2 \} & \to Tm^J \Gamma_1 \to Tm^J \Gamma_2 \to \text{Bool}
\end{align*}
\]

We have described the scoping rules but have not made much progress. Indeed two different but \(\alpha\)-equivalent terms can still distinguished. Worse,
by introducing environments and membership proofs as explicit objects, we have introduced new issues. Functions receiving terms now also receive or know the environment in which these terms are scoped. This extra information can be used by functions making them less agnostic to choices of free variables. Here are two functions using the environment by pattern-matching:

\[
\text{fast-fv} : \forall \{\Gamma\} \to \text{Tm}^J \Gamma \to \text{List Atom} \\
\text{fast-fv} \{\epsilon\} = [] \quad \text{-- for sure the term is closed} \\
\text{fast-fv} \quad t = \text{fv} \ t
\]

\[
\text{env-length} : \text{Env} \to \mathbb{N} \\
\text{env-length} \ (\epsilon) = 0 \\
\text{env-length} \ (\Gamma, \_ \ ) = 1 + \text{env-length} \ (\Gamma \ )
\]

\[
\text{env-length-Tm}^J : \forall \{\Gamma\} \to \text{Tm}^J \Gamma \to \mathbb{N} \\
\text{env-length-Tm}^J \{\Gamma\} = \text{env-length} \ (\Gamma \ )
\]

If one consider the term as the only input of \text{env-length-Tm}^J, then this function does not behave well since the same term can be scoped in two environments of different length. The issue is that \(\Gamma\) is a concrete input to the functions like \text{fv}, \text{ba}, \text{cmp-ba}, \text{fast-fv} and \text{env-length-Tm}^J.

In order to fix these issues we make use of abstract types and yet provide an interface with precise types for a safe usage. Environments (the type \text{Env}) are abstracted as so-called \textit{worlds}. Atoms used in binding positions are abstracted as so-called \textit{binders} and cannot even be compared. Atoms in free positions are glued together with the proof of their membership in the environment and are called \textit{names}. Finally a few extra operations allow to deal with these abstract types in a safe way.

### 2.2 NomPa: A programming interface in nominal style

Our approach is called \textsc{NomPa} and proposes a programming interface whose types are abstract. This interface (Figure 2.1) admits a concrete implementation (section 4.1). Hiding this implementation keeps the programmer away from the internal details and gives rise to interesting properties via parametricity.

While the complete interface is given in Figure 2.1, each ingredient of the interface is presented in turn. First here are the building blocks needed to define data types with names and binders in a nominal style.
## 2.2. NOMPA: A PROGRAMMING INTERFACE IN NOMINAL STYLE

record NomPa : Set₁ where
  constructor mk

  infixr 5 _≪_
  infix 3 _⊆_
  infix 2 _#_

field
  -- minimal kit to define types
  World : Set
  Name : World → Set
  Binder : Set
  _≪_ : Binder → World → World

  -- An infinite set of binders
  zeroB : Binder
  sucB : Binder → Binder

  -- Converting names and binders back and forth
  nameB : ∀ {α} → Name (b ≪ α)
  binderN : ∀ {α} → Name α → Binder

  -- There is no name in the empty world
  ∅ : World
  ¬Name∅ : ¬ (Name ∅)

  -- Names are comparable and exportable
  _≈=≈_ : ∀ {α} → x y : Name α → Bool
  exportN : ∀ {α} → Name (b ≪ α) → Name (b ≪ ∅) ⊎ Name α

  -- The fresh-for relation
  _#_ : Binder → World → Set
  _#∅_ : ∀ b → b # ∅
  suc# : ∀ {α} → b # α → (sucB b) # (b ≪ α)

  -- inclusion between worlds
  _⊆_ : World → World → Set
  coerceN : ∀ {α β} → (α ⊆ β) → (Name α → Name β)
  ⊆-refl : Reflexive _⊆_
  ⊆-trans : Transitive _⊆_
  ⊆-∅ : ∀ {α} → ∅ ⊆ α
  ⊆-≲ : ∀ {α β} → b → α ⊆ β → (b ≪ α) ⊆ (b ≪ β)
  ⊆-# : ∀ {α} → b # α → α ⊆ (b ≪ α)

Figure 2.1: The NOMPA interface
CHAPTER 2. THE NOMINAL APPROACH

2.2.1 All we need to define nominal syntax

To replace environments in the definition of well-scoped terms, we introduce an abstract notion of worlds. Hence the interface starts by an abstract type for worlds:

\[ \text{World} : \text{Set} \]

We consider it very important to highlight that atoms are used for distinct purposes whether they are in a binding position or a free position. We embrace that distinction and provide distinct types for these usages.

We first introduce a type for binders. Binders are atoms to be used only in binding positions. While these binders are explicitly accessible in terms it does not mean one can distinguish two \( \alpha \)-equivalent terms by simply looking at the binders. Indeed the interface does not provide any means to distinguish two binders. Internally binders are really atoms but the interface keeps them abstract:

\[ \text{Binder} : \text{Set} \]

For atoms to be put in free position, we introduce a type called \text{Name}. This type is indexed by a world in which the name is scoped. A name glues together an atom and a proof of its membership in the world:

\[ \text{Name} : \text{World} \rightarrow \text{Set} \]

Worlds can be thought of as a set of atoms (names or binders) but will be thought of as relations between names in section 4.3.

Now that we have binders and worlds, we can introduce a way to extend a world with a binder. This is analogous to the constructor \( \cdot \), of section 2.1.2 for extending an environment with an atom.

\[ \cdot \triangleleft \cdot : \text{Binder} \rightarrow \text{World} \rightarrow \text{World} \]

At this point, we have all we need to build data types with names and binders. The new definition of \( \text{Tm} \) is very close to the previous one. All we have to do is to use \( \cdot \triangleleft \cdot \) instead of \( \cdot \), rename \( \Gamma \) into \( \alpha \), and use \text{Name} instead of an atom plus a membership proof:

\[
\begin{align*}
\text{data } \text{Tm } \alpha & : \text{Set where} \\
V & : \text{Name } \alpha \rightarrow \text{Tm } \alpha \\
\cdot \triangleleft \cdot & : \text{Tm } \alpha \rightarrow \text{Tm } \alpha \rightarrow \text{Tm } \alpha \\
\lambda & : \forall b \rightarrow \text{Tm } (b \triangleleft \alpha) \rightarrow \text{Tm } \alpha \\
\text{Let} & : \forall b \rightarrow \text{Tm } \alpha \rightarrow \text{Tm } (b \triangleleft \alpha) \rightarrow \text{Tm } \alpha
\end{align*}
\]
Here binding constructs rely on dependent types, since the binder \( b \) is used in the type of the subterm. In our previous work [Pouillard and Pottier, 2010], we avoided dependent types on purpose to make the results more widely usable. The non-dependent approach based on links can be built on top of the one we are presenting here. A weak link [Pouillard and Pottier, 2010] from \( \alpha \) to \( \beta \) is represented by a binder \( b \) such that \( \beta = b \triangleleft \alpha \). Hence we want to first study in detail the dependent approach with its logical relation.

Here is a trivial example of a function that traverses a term and measures its size. It is remarkable for its simplicity: name abstractions are traversed without fuss. The code would be exactly the same in the bare nominal approach of section 2.1.1. In particular this unaltered induction suggests that the expressiveness with respect to the bare nominal approach is kept. It is efficient: no renaming, substitution, or shifting is involved. Polymorphic recursion is exploited: the call to \( \text{size } t \) in the \( \lambda \) (and \( \text{Let} \)) case is at some inner world.

\[
\begin{align*}
\text{size} : \ & \forall \{ \alpha \} \to \text{Tm } \alpha \to \mathbb{N} \\
\text{size } (V \_ ) & = 1 \\
\text{size } (t \cdot u) & = 1 + \text{size } t + \text{size } u \\
\text{size } (\lambda \_ t) & = 1 + \text{size } t \\
\text{size } (\text{Let } \_ t u) & = 1 + \text{size } t + \text{size } u
\end{align*}
\]

### 2.2.2 Building binders and names

In order to build terms, we need binders and names. Binders are introduced in our system using two simple primitive operations called \( \text{zero}^B \) and \( \text{suc}^B \):

\[
\begin{align*}
\text{zero}^B : & \text{Binder} \\
\text{suc}^B : & \text{Binder } \to \text{Binder}
\end{align*}
\]

We introduce a cheap convenience function to turn any natural number into a binder:

\[
\begin{align*}
_\mathbb{N} : & \mathbb{N} \to \text{Binder} \\
}\text{zero }^B = & \text{zero}^B \\
(\text{suc } n)^B = & \text{suc}^B (n^B)
\end{align*}
\]

In effect, binders are natural numbers with a limited interface. Here we give only zero and successor but all of the operations on natural numbers could be exposed as well. One key limitation, however, is that no information must leak out of a binder. Hence no equality test over binders is provided.
This is clarified when building the logical relation in section 4.3.

To build new names we provide a function, called $\text{name}^B$, to turn binders into names. For completeness we introduce the converse function $\text{binder}^N$. However, this function, without any properties on it, is of very little use.

\[
\begin{align*}
\text{name}^B & : \forall \{\alpha\} \ b \to \text{Name} (b \triangleleft \alpha) \\
\text{binder}^N & : \forall \{\alpha\} \to \text{Name} \alpha \to \text{Binder}
\end{align*}
\]

While $\text{name}^B$ can turn any binder into a name, it imposes the shape of the world that the produced name inhabits. Indeed $\text{name}^B b$ returns a name in any world whose last introduced binder is $b$. We will soon see that this is an important limitation and how to overcome it. For the moment, we have enough blocks to define a representation of the identity function!

\[
\begin{align*}
idTm & : \forall \{\alpha\} \to \text{Tm} \alpha \\
idTm = & \ x \ x \ (V (\text{name}^B \ x)) \\
& \text{where } x = 0^B
\end{align*}
\]

Our second example is a representation of the $\lambda$-term for false ($\lambda x. \lambda x. x$). We use the same binder twice on purpose to show a use of name shadowing. To type check the variable occurrence of $x$, the world $x \triangleleft \alpha$ is implicitly given to $\text{name}^B$ which returns a name in the world $x \triangleleft x \triangleleft \alpha$. Then each of the two “$\check{x} \ x$” takes away one “$x \triangleleft$” to leave the final term in $\alpha$.

\[
\begin{align*}
\text{falseTm} & : \forall \{\alpha\} \to \text{Tm} \alpha \\
\text{falseTm} = & \ x \ x \ (V (\text{name}^B \ x))) \\
& \text{where } x = 0^B \text{ and } y = 1^B
\end{align*}
\]

One however faces an issue when building a representation of the $\lambda$-term for true ($\lambda x. \lambda y. x$). The naïve approach does not type-check:

\[
\begin{align*}
\text{trueTm} & : \forall \{\alpha\} \to \text{Tm} \alpha \\
\text{trueTm} = & \ x \ x \ (\check{x} \ y \ (V (\text{name}^B \ x))) \\
& \text{where } x = 0^B \text{ and } y = 1^B
\end{align*}
\]

While $\text{name}^B \ x$ inhabits any world of the form $x \triangleleft \beta$, the context expects a name in the world $y \triangleleft x \triangleleft \alpha$. We introduce means to move a name from one world to another in section 2.2.3.

Closed terms The above well-typed terms ($idTm$ and $falseTm$) have no free variables. They are said to be closed. They both have the type:
∀ \{\alpha\} \rightarrow \text{Tm} \ \alpha. \ This \ world-polymorphic \ type \ reflects \ this \ closedness \ property. \ If \ any \ world \ fits, \ the \ empty \ world \ (noted \ \emptyset) \ fits \ as \ well. \ So \ \text{idTm} \ also \ has \ the \ type \ \text{Tm} \ \emptyset. \ Conversely, \ because \ the \ empty \ world \ is \ included \ in \ all \ worlds, \ we \ will \ be \ able \ to \ move \ any \ term \ from \ the \ empty \ world \ to \ an \ arbitrary \ world. \ In \ short \ \text{Tm} \ \emptyset \ and \ ∀ \{\alpha\} \rightarrow \text{Tm} \ \alpha \ are \ isomorphic \ types.

To \ allow \ exploiting \ the \ fact \ that \ any \ term \ in \ the \ empty \ world \ is \ closed, \ we \ introduce \ \neg \text{Name}\emptyset, \ which \ witnesses \ that \ there \ is \ no \ name \ in \ the \ empty \ world:

\emptyset : \text{World}
\neg\text{Name}\emptyset : \neg(\text{Name} \ \emptyset)

This \ last \ primitive \ operation \ is \ provided \ to \ secure \ the \ system \ against \ a \ buggy \ notion \ of \ closed \ terms \ but \ not \ only! \ In \ various \ situations \ it \ enables \ arguing \ that \ certain \ cases \ are \ impossible, \ like \ looking \ up \ a \ name \ in \ an \ empty \ environment.

### 2.2.3 World widening: Name weakening

It \ is \ often \ necessary \ to \ widen \ the \ world \ which \ a \ name \ inhabits. \ One \ example \ was \ the \ trueTm \ definition \ we \ tried \ earlier: \ to \ type-check \ it, \ we \ need \ to \ widen \ the \ world \ of \ the \ name \ x. \ Widening \ a \ world \ causes \ a \ loss \ of \ static \ information. \ For \ instance \ we \ have \ seen \ that \ a \ term \ in \ the \ empty \ world \ is \ closed: \ if \ one \ widens \ its \ world, \ it \ is \ no \ longer \ statically \ known \ to \ be \ closed. \ We \ call \ this \ operation \ weakening \ because \ it \ loses \ some \ static \ information. \ The \ name \ “weakening” \ is \ also \ vastly \ used \ for \ the \ same \ purpose \ on \ typing \ environments.

To \ account \ for \ the \ multiple \ ways \ in which \ we \ could \ widen \ a \ world \ we \ introduce \ a \ type \ to \ represent \ the \ inclusion \ between \ two \ worlds. \ The \ type \ \_
\subseteq \_ \ is \ for \ witnesses \ of \ world \ inclusion. \ If \ a \ world \ \alpha \ is \ included \ in \ a \ world \ \beta \ then \ it \ is \ permitted \ to \ transport \ a \ name \ (and \ a \ term \ as \ well, \ as \ we \ shall \ see) \ from \ \alpha \ to \ \beta. \ The \ primitive \ operation \ \text{coerce}^\wedge \ takes \ an \ inclusion \ witness, \ a \ name \ and \ it \ returns \ the \ same \ name \ at \ a \ wider \ world. \ We \ also \ introduce \ an \ alias \ to \ \text{coerce}^\wedge \ called \ \_
\because \_ \ which \ is \ useful \ to \ keep \ the \ code \ separated \ from \ the \ typing/proof: \ the \ proof, \ which \ appears \ between \ the \ angle \ brackets, \ can \ be \ safely \ skipped \ by \ the \ reader.

\_
\subseteq \_ : \text{World} \rightarrow \text{World} \rightarrow \text{Set}
\text{coerce}^\wedge : ∀ \{\alpha \ \beta\} \rightarrow \alpha \ \subseteq \ \beta \rightarrow (\text{Name} \ \alpha \rightarrow \text{Name} \ \beta)

infix 0 \_
\because \_
\(\because\): \(\forall \{\alpha \beta\} \rightarrow \text{Name} \alpha \rightarrow \alpha \subseteq \beta \rightarrow \text{Name} \beta\)

\(~\because~\text{n pf} = \text{coerce}^\#\text{pf n}\)

--- We can now write:
--- \(x \because\) some proof
--- Instead of the more noisy:
--- \(\text{coerce}^\#(\text{some proof}) x\)

**World inclusion rules** Rules for world inclusion are given in figure 2.1.
World inclusion is reflexive and transitive (\(\subseteq\text{-refl}\) and \(\subseteq\text{-trans}\)). The empty world \(\emptyset\) is a least element for world inclusion (\(\subseteq\emptyset\)). For any binder \(b\), \(b \triangleleft \_\) is covariant, meaning it preserves world inclusion (\(\subseteq\triangleleft\)).

Finally, the rule \(\subseteq\#\) states that a world \(\alpha\) is included into \(b \triangleleft \alpha\) under the condition that \(b\) is not a member of \(\alpha\). This condition is necessary to ensure the soundness of our library. An interpretation of worlds as sets suggests that this condition might be unnecessary. This shows the limitations of this way of thinking. When we introduce logical relations in section 4.3, we explain that interpreting worlds as *relations* provides a richer viewpoint and explains why this condition is necessary. The following code snippet demonstrates that without this condition one can write wrong programs:

```haskell
wrong : Binder \rightarrow Binder \rightarrow \text{Bool}
wrong x y = \text{name}^\# x ==^\# \text{name}^\# y \because\text{wrongProof} \)
where postulate
  wrongProof : y \triangleleft \emptyset \subseteq x \triangleleft y \triangleleft \emptyset
```

As this code snippet shows, in the absence of this condition it would be permitted to compare names at different worlds and so to compare binders and finally to make a distinction between two \(\alpha\)-equivalent terms.

**The fresh-for relation** The last inclusion rule \(\subseteq\#\), uses a fresh-for relation called \(\_\#.\_\). We introduce two rules to produce witnesses of this relation. The first rule tells that any binder is fresh for the empty world \((\_\#\emptyset)\). The second rule takes the “successor” of a fresh binder \((\text{suc}\#)\). This successor-based way of building new fresh-for witnesses is both simple and efficient. Indeed with these two rules, a binder is not only fresh for a world but strictly greater than any element of it, allowing for a constant time \text{suc}\# operation. These rules with their types can be found in figure 2.1 as well.

**Emptiness of worlds** The inclusion relation can express emptiness as well. A world \(\alpha\) is empty if it is included in the empty world. We use this definition of emptiness as opposed to an intensional equality with the empty world for two reasons. First \(\emptyset \subseteq \alpha\) is always true, hence the converse
is enough. Second we introduce in section 5.2 another operator on worlds called \( \# + 1 \) for which \( \emptyset \# + 1 \) is empty but does not reduce to \( \emptyset \).

With a backward reasoning, combining \texttt{coerce} and \( \neg \text{Name} \emptyset \) turns any contradiction on names into an inclusion problem, reusing any automation done on inclusion proofs.

\[
\neg \text{Name} : \forall \{ \alpha \} \to \alpha \subseteq \emptyset \to \neg (\text{Name} \alpha)
\]
\[
\neg \text{Name} \emptyset = \neg \text{Name} \emptyset \circ \text{coerce} \emptyset \subseteq \emptyset
\]

### Eliminating absurd names

We introduce convenient eliminators for absurd names which instead of going to the empty type, goes to any type of our choice:

\[
\text{Name-elim} : \forall \{ A : \text{Set} \} \{ \alpha \} \to \alpha \subseteq \emptyset \to \text{Name} \alpha \to A
\]
\[
\text{Name-elim \ pf \ x \ with \ \neg \text{Name} \ pf \ x} \quad \ldots \quad | ()
\]
\[
\text{Name-elim} \emptyset = \text{Name-elim} \subseteq \text{refl}
\]

### Relational reasoning

Sometimes one has to build complex inclusion witnesses. While inference would be of great effect here and is currently kept as future work, we propose a modest syntactic tool to build them, namely the \( \subseteq \text{-Reasoning} \) module. It gives access to the transitivity rule \( \subseteq \text{-trans} \) in a style which focuses more on the intermediate states of the reasoning rather than on the steps. The syntax is a list of worlds interspersed with inclusion witnesses, with \( \spadesuit \) after the last world. We soon present an example of its use with the function \texttt{trueTm}. The code for \( \subseteq \text{-Reasoning} \) is given below for reference and can be safely skipped.

\[
\text{module} \ \subseteq \text{-Reasoning} \ \text{where}
\]
\[
\text{infix} \ 2 \ \spadesuit
\]
\[
\text{infixr} \ 2 \ \subseteq (.)
\]
\[
\subseteq (.) : \forall \ {\alpha} \ {\beta \ \gamma} \to \alpha \subseteq \beta \to \beta \subseteq \gamma \to \alpha \subseteq \gamma
\]
\[
\subseteq (.) \ spadesuit = \subseteq \text{-trans}
\]
\[
\spadesuit : \forall \alpha \to \alpha \subseteq \alpha
\]
\[
\spadesuit = \subseteq \text{-refl}
\]
Building any term. We can now finally build all nominal terms (up to \(\alpha\)-equivalence). In section 3.2.8 we precisely show how to build all \(\lambda\)-terms by converting nominal \(\lambda\)-terms from section 2.1.1 to the type \(\text{Tm}\). Moreover we show an encoding for nominal types in section 6.5. In the meantime we focus on the term \(\text{trueTm}\). The two fresh-for rules above are the strict minimum for usability. More rules could be safely added but we focus on the minimal set of required rules here. The logical relation (section 4.2) serves as a criterion to judge what can or cannot be added. Having only these two rules imposes a particular style. A variable occurrence crosses only binders with a lower value to reach its own binder. This does not hinder much the expressiveness but requires to freshen some binders if one cannot prove they are fresh-for a given world. As stated previously removing this minor restriction would require adding more rules to the fresh-for and inclusion relations. One can finally build the term \(\text{trueTm}\):

\[
\text{trueTm} : \forall \{\alpha\} \to \text{Tm} \alpha \\
\text{trueTm} \{\alpha\} = x \ x \ (x \ y \ (V \ x \ N)) \\
\text{where } x = 0 \ B \\
y = 1 \ B \\
x \ N \ = \ \text{name}^B \ x \ (-\text{because } x \ \bigtriangleup \ 0 \ \subseteq \ (-\bigtriangleup \ # \ (\text{suc} \ (x \ # \ \emptyset)) \ ) \\
y \ \bigtriangleup \ x \ \bigtriangleup \ 0 \ \subseteq \ (-\bigtriangleup \ y \ (\bigtriangleup \ x \ \bigtriangleup \ 0)) \\
y \ \bigtriangleup \ x \ \bigtriangleup \ \alpha \ \bigtriangledown \ )
\]

The proof required to “move \(x\) in the correct world” is involved in comparison with the simplicity of the example. By choosing the empty world instead of world polymorphism we could cut in half the proof. To build larger examples, we build specialized building functions that requires only to specify the distance to the binding site [Pouillard, 2011a].

### 2.2.4 Comparing and refining names

While two binders cannot be compared, our interface allows comparing two names that inhabit a common world. This may seem contradictory, since one can turn binders into names. In fact, binder comparison cannot be implemented in terms of name comparison because two arbitrary binders can be turned only into names in distinct worlds.

\[
\text{==}^\text{N} : \forall \ {\alpha} \ (x \ y : \text{Name} \ \alpha) \to \text{Bool}
\]

While world inclusion gives a means to weaken the type of a name, we also need a means to strengthen the type of a name by refining its world. Assume a name \(x\) is known to be in the scope of a binder \(b\): \(x\) is in the world \(b \bigtriangleup \ \alpha\). The function \(\text{export}'\text{N}\) tests whether \(x\) is equal to \(b\); if so, \(x\) is refined to the world \(b \bigtriangleup \emptyset\) (which only \(b\) inhabits), otherwise it is refined
2.2. NOMPA: A PROGRAMMING INTERFACE IN NOMINAL STYLE

To α. In short given a name of type Name (b ◁ α), the function export^N returns the same name with a refined type telling whether the name stands on the b side or on the α side.

\[ \text{export}^N : \forall \{ b \alpha \} \to \text{Name (b ◁ α)} \to \text{Name (b ◁ ∅)} \sqcup \text{Name α} \]

\[ \text{export}^N = \text{maybe inj}_2 (\text{inj}_1 (\text{name}^B -)) \circ' \text{export}^N? \]

Actually the primitive operation in the interface is the function export^N? which returns a result of type Maybe (Name α). The function export^N is then built on top of export^N?.

\[ \text{-- A →? B is the type of partial functions from A to B} \]
\[ A \to? B = A \to \text{Maybe B} \]

\[ \text{export}^N? : \forall \{ b \alpha \} \to \text{Name (b ◁ α)} \to? \text{Name α} \]

On top of export^N? we also build a convenient eliminator for names which is simply the elimination of the result of export^N?.

\[ \text{exportWith} : \forall \{ b \alpha A \} \to A \to (\text{Name } \alpha \to A) \to \text{Name (b ◁ α)} \to A \]
\[ \text{exportWith } v f = \text{maybe } f \nu \circ' \text{export}^N? \]
Chapter 3

Programming on top of NomPa

3.1 Various examples

3.1.1 Example: computing free variables

We now have enough tools to present a more interesting example, namely a function that constructs a list of the free variables of a term. At variables and applications, the code is straightforward. At a name abstraction, one easily collects the free variables of the body via a recursive call. However, this yields a list of names that inhabit the inner world of the abstraction—a value of type \( \text{List} (\text{Name} (b \triangleleft \alpha)) \). This list cannot be directly returned, and this is fortunate, since doing so would let the bound name leak out of its scope! We define an auxiliary function, \( \text{rm} \), which removes all occurrences of a binder \( b \) in a list of names and at the same time performs type refinement in the style of \( \text{export}^\mathbb{N}/\text{export}^\mathbb{N} \).

\[
\begin{align*}
\text{rm} & : \forall \{ \alpha \} \ b \rightarrow \text{List} (\text{Name} (b \triangleleft \alpha)) \rightarrow \text{List} (\text{Name} \alpha) \\
\text{rm} \ b \ [] & = [] \\
\text{rm} \ b \ (x :: xs) \ & \text{with} \ \text{export}^\mathbb{N} x \ -- \ b \ \text{is implicit} \\
& \ldots \ (\sim \ \text{bound: } x \equiv b -) \ | \ \text{inj}_1 \ _x & = \text{rm} \ b \ xs \\
& \ldots \ (\sim \ \text{free: } x \not\equiv b -) \ | \ \text{inj}_2 x' & = x' :: \text{rm} \ b \ xs
\end{align*}
\]

\[
\begin{align*}
\text{fv} & : \forall \{ \alpha \} \rightarrow \text{Tm} \ \alpha \rightarrow \text{List} (\text{Name} \ \alpha) \\
\text{fv} (V \ x) & = [ \ x \ ] \\
\text{fv} (\text{fct} \cdot \arg) & = \text{fv} \ \text{fct} ++ \text{fv} \ \text{arg} \\
\text{fv} (\forall \ b \ t) & = \text{rm} \ b \ (\text{fv} \ t) \\
\text{fv} (\text{Let} \ b \ t \ u) & = \text{fv} \ t ++ \text{rm} \ b \ (\text{fv} \ u)
\end{align*}
\]

The function \( \text{rm} \) applies \( \text{export}^\mathbb{N} \) to every name \( x \) in the list and builds
a list of only those \( x \)'s that successfully export to the world \( \alpha \). It exhibits a typical way of using \( \text{export}^N \) to perform a name comparison together with a type refinement. This idiom is recurrent in the programs that we have written.

### 3.1.2 Example: working with environments

Here is another example, where we introduce the use of an environment.

```haskell
occurs : \( \forall \{ \alpha \} \rightarrow \text{Name} \alpha \rightarrow \text{Tm} \alpha \rightarrow \text{Bool} \)
occurs \( x_0 \) = occ ( \( \lambda y \rightarrow x_0 =^N y \) )

where

- \( \text{OccEnv} : \text{World} \rightarrow \text{Set} \)
- \( \text{OccEnv} \alpha = \text{Name} \alpha \rightarrow \text{Bool} \)
- \( \text{extend} : \forall \{ \alpha b \} \rightarrow \text{OccEnv} \alpha \rightarrow \text{OccEnv} (b \triangleleft \alpha) \)
- \( \text{extend} = \text{exportWith} \text{false} \)

\( \text{occ} : \forall \{ \alpha \} \rightarrow \text{OccEnv} \alpha \rightarrow \text{Tm} \alpha \rightarrow \text{Bool} \)
\( \text{occ} \Gamma (V x) = \Gamma x \)
\( \text{occ} \Gamma (t \cdot u) = \text{occ} \Gamma t \lor \text{occ} \Gamma u \)
\( \text{occ} \Gamma (\lambda \_ t) = \text{occ} (\text{extend} \Gamma) t \)
\( \text{occ} \Gamma (\text{Let} \_ t u) = \text{occ} \Gamma t \lor \text{occ} (\text{extend} \Gamma) u \)
```

The function \( \text{occurs} \) tests whether the name \( x_0 \) occurs free in a term. An environment \( \Gamma \) is carried down, augmented when a binder is crossed, and looked up at variable occurrences. Here, this environment is represented as a function of type \( \text{Name} \alpha \rightarrow \text{Bool} \). Although this is a simple and elegant representation, others exist. For instance, we could represent the environment as a list of binders: the code for this variant is online [Pouillard, 2011a]; see also below.

The definition of \( \text{extend} \) states that, in order to look up \( x \) in the environment \( \text{extend} \Gamma \), one must first compare \( x \) and \( b \) and, only if they differ, one must look up \( x \) in \( \Gamma \). If \( x \) and \( b \) are equal, then this occurrence of \( x \) is not free, so \( \text{occ} \Gamma (V x) \) must return \text{false}. This is concisely implemented by using the function \( \text{exportWith} \) built on top of \( \text{export}^N \) (Again thanks to the precise typing using worlds, \( b \) is passed as an implicit argument to the function \( \text{extend} \) and \( \text{exportWith} \)).

We claim that this code is standard and uncluttered. There is no hidden cost: no renaming is involved. Admittedly, neither functions nor lists are the most efficient representation of environments. It would be nice to be able to implement environments using, say, balanced binary search trees, while preserving well-typedness. We leave this issue to future study.

The type system forces us to use names in a sound way. For instance, in the definition of \( \text{occ} \), forgetting to extend the environment when crossing a
3.1. VARIOUS EXAMPLES

binder (that is, writing \( \Gamma \) instead of extend \( \Gamma \)) would cause a type error. In the definition of extend, attempting to check whether \( x \) occurs in \( \Gamma \) without first comparing \( x \) and \( b \) would cause a type error. Remember that in this nominal implementation scheme it is permitted for newer bindings to shadow earlier ones; our type discipline guarantees that the code works also in that case.

As suggested previously, one may wish to represent environments as an explicit data structure (an association list keyed by binders) rather than as an opaque object (a lookup function).

\[
\text{data DataEnv } (A : \text{Set}) : (\alpha \beta : \text{World}) \to \text{Set where}
\quad \epsilon : \forall \{\beta\} \to \text{DataEnv } A \beta \beta
\quad \_ : \_ \_ : \forall \{\alpha \beta\} (\Gamma : \text{DataEnv } A \alpha \beta) \ b \ (x : A) \\
\to \text{DataEnv } A \ (b \triangleleft \alpha) \beta
\]

\[
\text{lookup } : \forall \{A \alpha \beta\} \to \text{DataEnv } A \alpha \beta \to \text{Name } \alpha \to \text{Name } \beta \cup A
\quad \epsilon \ = \ \text{inj}_1
\quad \text{lookup } \ (\Gamma , \_ \_ \_ \_ v) = \text{exportWith } (\text{inj}_2 \ v) \ (\text{lookup } \Gamma)
\]

The type DataEnv \( A \alpha \beta \) is the type of an environment, or environment fragment, where \( \alpha \) is called the inner world, where \( \beta \) is called the outer world, and every name in the environment is associated with a datum of type \( A \). The inner world is the world where all the binders of the environment are in scope. The outer world is the world where none of the binders are in scope. The expression lookup \( \Gamma x \) looks up the name \( x \) in the environment \( \Gamma \). The name \( x \) must make sense in the scope of \( \Gamma \), that is, \( x \) must inhabit the world \( \alpha \). If \( x \) is found among the bindings, then the information associated with \( x \) can be returned. If \( x \) is not found among the bindings, then \( x \) is returned, with a more precise type: indeed, since \( x \) is not among the names introduced by \( \Gamma \), it must make sense outside \( \Gamma \), that is, in the world \( \beta \).

We illustrate the use of DataEnv with an alternative definition of the function \( \text{fv} \) (here the payload type parameter \( A \) is instantiated with the unit type \( \top \)). This variant avoids the need to take the bound atoms off the list by not inserting them in the first place. At variables, we use lookup to check whether the name is free or bound. If the name is free, we return it as a singleton list (using \([\_])\). If it is bound, we ignore it and return an empty list. At every other node, we simply carry out a recursive traversal. Whenever a name abstraction is entered, the current environment \( \Gamma \) is extended with the bound name \( b \).
3.1.3 Example: Term comparison

Our next example focuses on comparison of terms. We first define \( |\text{Cmp}| \), where \( |\text{Cmp}| F \) is the type of functions comparing \( F \)-structures. In our case the index type \( Ix \) is the type of worlds: \( \text{World} \).

\[
|\text{Cmp}| : \forall \{Ix\} (F : Ix \to \text{Set}) (i j : Ix) \to \text{Set}
\]

\( |\text{Cmp}| F \ i \ j = F \ i \to F \ j \to \text{Bool} \)

To compare two terms we carry down an environment, telling how to compare two names. At name occurrences we ask our environment, at application nodes we carry down our environment, and we need to extend the environment at name-abstractions. We extend the environment with the function \( \text{extendNameCmp} \) which receives a name comparator \( f \) for worlds \( \alpha _1 \) and \( \alpha _2 \), a name \( x_1 \) in \( b_1 \triangleleft \alpha _1 \), and a name \( x_2 \) in \( b_2 \triangleleft \alpha _2 \). Then, the function \( \text{extendNameCmp} \) exports both names \( x_1 \) and \( x_2 \) simultaneously: when the two exports succeed we can use the comparator \( f \), when both fail we learn that \( x_1 \) is \( b_1 \) and that \( x_2 \) is \( b_2 \) we hence return \text{true}, when one succeeds and the other fails we return \text{false}:

\[
\text{extendNameCmp} : \forall \{\alpha _1 \alpha _2 b_1 b_2\} \to |\text{Cmp}| \text{Name} \alpha _1 \alpha _2
\]

\[
\text{extendNameCmp} f \ x_1 \ x_2 \text{ with export}^b? \ x_1 \ | \text{export}^b? \ x_2
\]

\[
\ldots \ | \text{just } x_1' \ | \text{just } x_1' = f \ x_1' \ x_1'
\]

\[
\ldots \ | \text{nothing} \ | \text{nothing} = \text{true}
\]

\[
\ldots \ | \_ \ | \_ = \text{false}
\]

\[
\text{cmpTm} : \forall \{\alpha _1 \alpha _2\} (\Gamma : |\text{Cmp}| \text{Name} \alpha _1 \alpha _2) \to \text{Tm} \alpha _1 \to \text{Tm} \alpha _2 \to \text{Bool}
\]
3.2. KITS AND TRAVERSALS

\[
\text{cmpTm } \Gamma (V \ x_1) (V \ x_2) = \Gamma \ x_1 \ x_2
\]
\[
\text{cmpTm } \Gamma (t_1 \cdot u_1) (t_2 \cdot u_2) = \text{cmpTm } \Gamma t_1 \ t_2 \land \text{cmpTm } \Gamma u_1 \ u_2
\]
\[
\text{cmpTm } \Gamma (x \_ \ t_1) (x \_ \ t_2) = \text{cmpTm } (\text{extendNameCmp } \Gamma) t_1 \ t_2
\]
\[
\text{cmpTm } (\text{Let } b_1 t_1 u_1) (\text{Let } b_2 t_2 u_2) = \text{cmpTm } \Gamma t_1 \ t_2 \land \text{cmpTm } (\text{extendNameCmp } \Gamma) u_1 \ u_2
\]
\[
\text{cmpTm } _- _- = \text{false}
\]

Notice that the code above does not need to compare neither names nor binders from the first term with those from the second term. Two bound names are said to be equal when they are bound at the same time. Bound names are said to be compared positionally. This also explains why we do not need a function to compare binders. Notice also that the function \(\text{cmpTm}\) has to accept two terms in different worlds to carry the recursion successfully. In the end we can give the function \(\_\_\_\text{==}\_\_\_\) as an initial environment yielding an homogeneous comparison on terms, which coincides with \(\alpha\)-equivalence:

\[
\_\_\_\text{==}\_\_\_ : \forall \{\alpha\} \to \text{Tm } \alpha \to \text{Tm } \alpha \to \text{Bool}
\]
\[
\_\_\_\text{==}\_\_\_ = \text{cmpTm } \_\_\_\text{==}\_\_\_\text{N}
\]

In this final setting bound names are compared positionally and free names are compared for equality.

3.2 Kits and Traversals

We have seen that working with worlds requires explicitly moving names from world to world using operations like \(\text{coerce}^N\) and \(\text{export}^N\). These operations quickly become necessary at the level of user-defined types like our type \(\text{Tm}\). More generally any operation on names would benefit from being lifted to user-defined types.

From our experimentations with this library we outline two points. First, in most of the operations on terms we present, only the binding structure is relevant. The code for the traversal can hence be written only once. Second, the parts specific to each operation can be made reusable to work not only with the generic traversal but with custom traversals as well.

To share code and separate concerns we introduce some infrastructure. While abstract this infrastructure is then concretely applied to our example type \(\text{Tm}\).

3.2.1 Traversal Kits

We first introduce the notion of traversal kits, which encompasses: a type of environment \(\text{Env } \alpha \ \beta\) to be carried down in the traversal going from the world \(\alpha\) to \(\beta\); a function \(\text{trName}\) to apply the environment at names; a function \(\text{trBinder}\) for binders; and finally a function \(\text{extEnv}\) to push
CHAPTER 3. PROGRAMMING ON TOP OF NOMPA

an environment under a binder. For more flexibility the result type Res of trName is a parameter as well, we shall see its use later on in this section. We build traversal kits for: coercing (applying a world inclusion witness), exporting, applying general effectful functions over names, freshening, and combinations of these.

record TrKit (Env : (α β : World) → Set)
    (Res : World → Set) : Set where
  constructor mk
  field
    trName : ∀ {α β} → Env α β → Name α → Res β
    trBinder : ∀ {α β} → Env α β → Binder → Binder
    extEnv : ∀ {α β} b (∆ : Env α β)
      → Env (b ◁ α) (trBinder ∆ b ◁ β)

3.2.2 Coercing kit

Our first kit, called coerceKit, is simple and to the point. The “environment” type is _≤_. The result type is simply Name. The operation to call at names is coerceN. The action at binders is the identity, meaning that this kit does not perform any renaming or freshening. Finally the inclusion rule _≤-◁_ fits the job of extEnv.

coerceKit : TrKit _≤_ Name
coerceKit = mk coerceN (const id) _≤-◁

To illustrate the usage of coerceKit, we use it to lift coerceN from names to terms. In this situation the reuse is negligible, but this code serves a pedagogical purpose.

module CoerceTmWithCoerceKit where
  open TrKit coerceKit

  coeTm : ∀ {α β} → α ≤ β → Tm α → Tm β
  coeTm Δ (V x) = V (trName Δ x)
  coeTm Δ (t · u) = coeTm Δ t · coeTm Δ u
  coeTm Δ (ƛ b t) = ƛ (trBinder Δ b) (coeTm (extEnv b Δ) t)
  coeTm Δ (Let b t u) = Let (trBinder Δ b) (coeTm Δ t)
    (coeTm (extEnv b Δ) u)

  The function coeTm takes an inclusion witness and an input term. The inclusion witness is carried down the traversal, used at names with the function trName (equal to coerceN in the coerceKit) and extended at abstrac-
3.2. KITS AND TRAVERSALS

functions with the function \texttt{extEnv} (equal to \(\subseteq\) in the \texttt{coerceKit}). The function \texttt{trBinder} is used to choose the binders of the output term which are the ones from the input in the \texttt{coerceKit}. This traversal is actually independent of the kit we use.

Our next kit requires the concept of name supplies. A name supply for the world \(\alpha\) is just a pair of a binder called \texttt{seed} and a proof that \texttt{seed} is fresh for \(\alpha\):

\[
\text{record Supply } \alpha : \text{Set where}
\begin{align*}
\text{constructor } & \_ \_ \\
\text{field} & \\
\text{seed}^\beta : \text{Binder} \\
\text{seed}# : \text{seed}^\beta \# \alpha
\end{align*}
\]

We also introduce two helpers called \texttt{zero}\(^\alpha\) and \texttt{suc}\(^\alpha\). \texttt{zero}\(^\alpha\) is the initial name supply and the function \texttt{suc}\(^\alpha\) increments both the seed and the fresh-for proof:

\[
\begin{align*}
\text{zero}\(^\alpha\) & : \text{Supply } \emptyset \\
\text{zero}\(^\alpha\) & = 0^\beta , 0^\beta \#\emptyset \\
\text{suc}\(^\alpha\) & : \forall \{\alpha\} \to (s : \text{Supply } \alpha) \to \text{Supply } (\text{Supply}.\text{seed}^\beta s \triangleleft \alpha) \\
\text{suc}\(^\alpha\)(seed^\beta , seed#) & = \text{suc}^\beta \text{seed}^\beta , \text{suc}# \text{seed}#
\end{align*}
\]

3.2.3 Renaming kits

Our second kit, the “renaming kit”, is more involved and shows how to apply any function over names on the binding structure. To avoid captures we have to freshen the binders in the result and the system indeed imposes that we do so. We first define the record type \texttt{SubstEnv} \(\alpha \beta\). This record type holds: a function \texttt{trName} to apply at names and a name supply for \(\beta\):

\[
\text{record SubstEnv } (\text{Res} : \text{World } \to \text{Set}) \alpha \beta : \text{Set where}
\begin{align*}
\text{constructor } & \_ \_ \\
\text{field} & \\
\text{trName} : \text{Name } \alpha \to \text{Res } \beta \\
\text{supply} : \text{Supply } \beta
\end{align*}
\]

\[
\text{open Supply supply public}
\]

\[
\begin{align*}
\text{-- each binder is translated to a fresh binder} \\
\text{trBinder : } & \text{Binder } \to \text{Binder} \\
\text{trBinder } \_ & = \text{seed}^\beta
\end{align*}
\]
The so-called renameKit is then defined by providing \( \text{trName}, \text{trBinder} \) and \( \text{extEnv} \). This last one is the most involved part of the kit and depicted in figure 3.1. The function \( \text{trName} \) is lifted using \( \text{exportWith} \). The lifted function \( \text{trName} \) takes a name, if this name is bound then the \( \text{seed}^B \) is returned, otherwise this name (exported) is given to \( \text{trName} \) to produce a name which is then imported back using \( \text{coerce}^N \). This call to \( \text{coerce}^N \) is valid only because \( \text{seed}^B \) is known to be fresh for the output world. Here again \( \text{SubstEnv} \) is parameterized by the result type of \( \text{trName} \) for greater flexibility:

\[
\begin{align*}
\text{RenameEnv} & : (\alpha \beta : \text{World}) \rightarrow \text{Set} \\
\text{RenameEnv} & = \text{SubstEnv} \text{Name} \\
\text{renameKit} & : \text{TrKit RenameEnv Name} \\
\text{renameKit} & = \text{mk trName trBinder extEnv} \\
\text{where} & \\
\text{open SubstEnv} & \\
\text{extEnv} & : \forall \{\alpha \beta\} \ b \ (\Delta : \text{RenameEnv} \alpha \beta) \rightarrow \text{RenameEnv} (b \triangleleft \alpha) (\_ \triangleleft \beta) \\
\text{extEnv} & = (\text{trName'}, (\text{seed}^B, \text{seed}^#\beta)) \\
\text{where} & \\
\text{trName'} & = \text{exportWith} \\
& (\text{name}^B \text{seed}^B) \quad \text{-- bound} \\
& (\text{coerce}^N (\subseteq^# \text{seed}^#\beta \circ \text{trName}) \quad \text{-- free})
\end{align*}
\]

Our renaming kit works for any total function over names. However, to lift the function \( \text{export}^B \) from names to terms, we need to deal with partial functions as well. We can actually build another renaming kit parameterized over a notion of effectful computation, namely an applicative functor. An applicative functor [McBride and Paterson, 2008] is halfway
3.2. KITS AND TRAVERSALS

between a functor and a monad. Like a monad, an applicative functor has a unit called pure. The function pure allows to embed any pure value as a potentially effectful one. The second operation, called \_\_\_\_, is an effectful application, taking an effectful function and argument and resulting in an effectful result. Here is how we can use applicative functors to apply an effectful function to a list:

```haskell
module MapA {E} (E-app : Applicative E) where
  open Applicative E-app

  mapA : {A B : Set} → (A → E B) → List A → E (List B)
  mapA _ [] = pure []
  mapA f (x :: xs) = pure _:_ ⊗ f x ⊗ mapA f xs
```

To build a more general renaming kit, we reuse the type SubstEnv but make use of the flexibility on the result type to plug in the effect type E (the applicative functor). The code for renameAKit is similar to renameKit, so we omit it here and provide only its type:

```haskell
RenameAEnv : (E : Set → Set) (α β : World) → Set
RenameAEnv E = SubstEnv (E ◦ Name)

renameAKit : ∀ {E} → Applicative E →
    TrKit (RenameAEnv E) (E ◦ Name)
renameAKit = {! code similar to renameKit omitted !}
```

3.2.4 Substitution kit

We reuse our SubstEnv once more to generalize in another direction the renaming kit to the so-called substKit which helps build substitution functions. Substitution functions are built for a structure F (like our type Tm), provided there is a way of injecting names to F-structures and of coercing an F-structure from one world to another. Here again we choose another result type for SubstEnv, namely F :

```haskell
-- Index-respecting functions
F \rightarrow\| G = ∀ {i} → F i → G i

-- The type for ‘coerce’ on an F-structure
Coerce F = ∀ {α β} → α ≺ β → F α → F β

substKit : ∀ {F}
3.2.5 Other kits and combinators

We can also build other kits and combinators [Pouillard, 2011a]. For instance $\circ$-Kit can compose two kits by pairing the two environments and composing their operations. Another combinator, starKit, takes a kit $k$ on environments of type $Env$ and builds a kit working on $Star\ Env$ (the reflexive and transitive closure operator in Agda). Finally with mapKit one can pre-compose and post-compose a function with a kit to get a new kit. This last one is given below:

```agda
mapKit : \forall \{Env F G\} \{f : Name \to\ Name\} \{g : F \to\ G\}
        \to TrKit Env F \to TrKit Env G
mapKit f g kit = mk (\lambda \Delta \to g \circ trName \Delta \circ f) trBinder extEnv
where open TrKit kit
```

3.2.6 Reusable traversal

Putting all these kits to work is a matter of writing a traversal function working for any kit and any effect. It is essentially a map function where the free names are transformed by a user-supplied function. More precisely the function trTm traverses the term, carrying an environment. It uses trName at variable occurrences without putting back the constructor V. In every other case, it just rebuilds the same structure using the corresponding constructor and the operations of our applicative functor. To carry the environment under bindings extEnv is used:

```agda
mapKit : \forall \{Env F G\} \{f : Name \to\ Name\} \{g : F \to\ G\}
        \to TrKit Env F \to TrKit Env G
mapKit f g kit = mk (\lambda \Delta \to g \circ trName \Delta \circ f) trBinder extEnv
where open TrKit kit
```
3.2. KITS AND TRAVERSALS

module TraverseTm {E} (E-app : Applicative E) {Env} (trKit : TrKit Env (E ◦ Tm)) where

open Applicative E-app
open TrKit trKit

trTm : ∀ {α β} → Env α β → Tm α → E (Tm β)
trTm Δ (V x) = trName Δ x
trTm Δ (t · u) = pure _ _ ⊙ trTm Δ t ⊙ trTm Δ u
trTm Δ (λ b t) = pure (λ _) ⊙ trTm (extEnv b Δ) t
trTm Δ (Let b t u) = pure (Let _) ⊙ trTm Δ t ⊙ trTm (extEnv b Δ) u

3.2.7 Reusing the traversal

We can now collect the fruit of our work, by combining the traversal and a few kits. For the sake of simplicity we directly do so on the type Tm, but in our development [Pouillard, 2011a] we further abstract over Tm (as F) and trTm by defining a sequence of parameterized modules.

open TraverseTm

-- Like ‘trTm’ but restores the constructor ‘V’.
-- The result type of ‘trKit’ is refined.
trTm’ : ∀ {E} (E-app : Applicative E) {Env} (trKit : TrKit Env (E ◦ Name)) {α β} → Env α β → Tm α → E (Tm β)
trTm’ E-app trKit = trTm E-app (mapKit id (Applicative._<$>_ E-app V) trKit)

While coerceTm can be lifted to terms using a renaming function, this would impose freshening. Using trTm’ with the coerceKit yields a more efficient implementation.

-- The identity on types from an applicative functor
id-app : Applicative id
id-app = {! definition omitted !}

coerceTm : ∀ {α β} → α ⊆ β → Tm α → Tm β
coerceTm = trTm’ id-app coerceKit

Building the renaming function amounts to use one of our renaming kits
and to pick one applicative functor:

\[
\text{renameTmA} : \forall \{E\} \to \text{Applicative } E \to
\forall \{\alpha \beta\} \to \text{Supply } \beta \to (\text{Name } \alpha \to E (\text{Name } \beta)) \to (\text{Tm } \alpha \to E (\text{Tm } \beta))
\]

\[
\text{renameTmA } E\text{-app } s \ f = \text{trTm'} E\text{-app } (\text{renameAKit } E\text{-app}) (f \ , \ s)
\]

\[
\text{renameTm} : \forall \{\alpha \beta\} \to \text{Supply } \beta \to (\text{Name } \alpha \to \text{Name } \beta) \to (\text{Tm } \alpha \to \text{Tm } \beta)
\]

\[
\text{renameTm } s \ f = \text{trTm'} \text{id-app } \text{renameKit } (f \ , \ s)
\]

\[
\text{renameTm?} : \forall \{\alpha \beta\} \to \text{Supply } \beta \to (\text{Name } \alpha \to ? \text{Name } \beta) \to (\text{Tm } \alpha \to ? \text{Tm } \beta)
\]

\[
\text{renameTm?} = \text{renameTmA } \text{Maybe.applicative}
\]

Exporting is built by lifting the function \text{export}_N \? using the function \text{renameTm}?:

\[
\text{exportTm?} : \forall \{b \alpha\} \to \text{Supply } \alpha \to \text{Tm } (b \triangleleft \alpha) \to ? \text{Tm } \alpha
\]

\[
\text{exportTm? } s = \text{renameTm? } s \ \text{export}_N \?
\]

Another special case of \text{renameTm?} is the so-called \text{closeTm}?. This function takes a term in any world and checks if the term is closed. If so, the same term is returned in the empty world. Otherwise the function fails by returning \text{nothing}:

\[
\text{closeTm?} : \forall \{\alpha\} \to \text{Tm } \alpha \to ? \text{Tm } \emptyset
\]

\[
\text{closeTm?} = \text{renameTm? } (0^B \ , \ (0^B)\#\emptyset) \ (\text{const nothing})
\]

Building capture avoiding substitution amounts to use the substitution kit with the constructor \text{V} and the function \text{coerceTm} as arguments:

\[
\text{substTm} : \forall \{\alpha \beta\} \to \text{Supply } \beta \to (\text{Name } \alpha \to \text{Tm } \beta) \to \text{Tm } \alpha \to \text{Tm } \beta
\]

\[
\text{substTm } (s \ , \ s\#) \ f = \text{trTm } \text{id-app } (\text{substKit } \text{V } \text{coerceTm}) (f \ , \ s \ , \ s\#)
\]

To illustrate the use of \text{substTm}, here is a simple function \text{\beta-red} which performs a \beta-reduction when a \beta-redex appears at the root of the term. The function \text{exportWith } a \text{ V} associate \text{a} to \text{b} and \text{x to V x} when \text{x \neq b}:

\[
\text{\beta-red } : \forall \{\alpha\} \to \text{Supply } \alpha \to \text{Tm } \alpha \to \text{Tm } \alpha
\]

\[
\text{\beta-red } s \ (x \ b \ f \cdot \ a) = \text{substTm } s \ (\text{exportWith } a \text{ V}) \ f
\]

\[
\text{\beta-red } _t = t
\]
3.2. KITS AND TRAVERSALS

3.2.8 Building any λ-term

A way to illustrate that every λ-term can be encoded using our type \( Tm \) is to define a conversion function from another type for λ-terms to the type \( Tm \). We do so by choosing the type \( Tm^A \) from section 2.1.1 as the source language.

The process is very close to the combination of a specific renaming kit and traversal function. The kit is specific since the source names are of type \( Atom \) and not \( Name \). The traversal function is specific since the source and target types are not the same and we picked the identity functor for simplicity.

First, we introduce the environment type which holds a mapping from free atoms to free names and a name supply:

\[
\text{module Conv-Tm}^A \rightarrow Tm \text{ where}
\]
\[
\text{record Env } \alpha \text{ : Set where}
\]
\[
\text{constructor } \_ \_ \_
\]
\[
\text{field}
\]
\[
\trAtom : \text{Atom } \rightarrow \text{Name } \alpha
\]
\[
\text{supply : Supply } \alpha
\]
\[
\text{open Supply supply public}
\]
\[
\text{open Env}
\]

We then define how an environment is extended. It works similarly to the one for the renaming kit:

\[
\text{extEnv} : \forall \{ \alpha \} \rightarrow \text{Atom } \rightarrow (\Delta : \text{Env } \alpha) \rightarrow \text{Env } (\text{seed}^B \Delta \circ \alpha)
\]
\[
\text{extEnv } b^A \Delta = \text{tr}^N, \text{ suc}^\#(\text{supply } \Delta)
\]
\[
\text{where } \text{tr}^N = \lambda x^A \rightarrow \text{if } b^A = x^A \text{ then } \text{name}^B(\text{seed}^B \Delta)
\]
\[
\text{else } \text{coerce}^\#(\subseteq^\#(\text{seed}^\# \Delta)) (\text{trAtom } \Delta x^A)
\]

The following function \( \text{conv} \) is then straightforward, calling \( \text{trAtom} \) on atoms at the variable case and using \( \text{extEnv} \) when crossing a binding. This function \( \text{conv} \) is simpler than the traversal function seen previously since we avoided the use of effectful computations, however the applicative version works as well. The function \( \text{conv} \) can then be used if we can associate all atoms to names and have the corresponding name supply.

\[
\text{conv} : \forall \{ \alpha \} \rightarrow \text{Env } \alpha \rightarrow \text{Tm}^A \rightarrow \text{Tm } \alpha
\]
\[
\text{conv } \Delta (V x) = V (\text{trAtom } \Delta x)
\]
\[
\text{conv } \Delta (x^B b^A t) = x^B (\text{conv } (\text{extEnv } b^A \Delta) t)
\]
\[
\text{conv } \Delta (t \cdot u) = \text{conv } \Delta t \cdot \text{conv } \Delta u
\]
\[
\text{conv } \Delta (\text{Let } b^A t u) = \text{Let } \_ ((\text{conv } \Delta t) (\text{conv } (\text{extEnv } b^A \Delta) u))
\]
To convert closed terms we need an empty environment. However the type $Tm^A$ does not ensure closedness. Hence the conversion is partial. To build this partial conversion we define it in two steps. The first step uses the function $conv$ with an empty environment. This empty environment maps any atom to the name $0^R$, the name supply hence starts at $1^R$. As the second step we use the function $closeTm?$ which strengthens the type of the input term if it is closed and fails otherwise.

\[
\begin{align*}
\text{emptyEnv} & : \text{Env} (0^B \triangleleft \emptyset) \\
\text{emptyEnv} & = \text{const} (0^R), \text{ suc}^g \text{ zero}^g
\end{align*}
\]

\[
\begin{align*}
conv{}? & : Tm^A \rightarrow? Tm \emptyset \\
conv{}? & = closeTm? \circ conv \text{ emptyEnv}
\end{align*}
\]

### 3.3 Towards elaborate uses of worlds

#### 3.3.1 Data type of “one hole contexts”

The type $Tm$ is just one basic example of an algebraic data type that involves names and binders. As a more challenging example, consider a type $C$ of one-hole contexts associated with $Tm$. The type $C$ is indexed with two worlds, which respectively play the role of an outer world and an inner world. The idea is, plugging a term of type $Tm \beta$ into the hole of a context of type $C^\alpha \beta$ produces a term of type $Tm^\alpha$. The definition of the type $C$ is as follows:

\[
\begin{align*}
data C^\alpha : \text{World} \rightarrow \text{Set where} \\
\text{Hole} & : C^\alpha \alpha \\
{}^-1_\alpha & : \forall \{\beta\} \rightarrow C^\alpha \beta \rightarrow Tm^\alpha \rightarrow C^\alpha \beta \\
{}^-2_\alpha & : \forall \{\beta\} \rightarrow Tm^\alpha \rightarrow C^\alpha \beta \rightarrow C^\alpha \beta \\
\chi & : \forall \{\beta\} \ b \rightarrow C^\alpha (b \triangleleft \alpha) \beta \rightarrow C^\alpha \beta \\
\text{Let}_1 & : \forall \{\beta\} \ b \rightarrow C^\alpha \beta \\
& \quad \quad \rightarrow Tm^\alpha (b \triangleleft \alpha) \rightarrow C^\alpha \beta \\
\text{Let}_2 & : \forall \{\beta\} \ b \rightarrow Tm^\alpha \\
& \quad \quad \rightarrow C^\alpha (b \triangleleft \alpha) \beta \rightarrow C^\alpha \beta
\end{align*}
\]

Contexts bind names: the hole can appear under one or several binders. This is why, in general, a context has distinct outer and inner worlds. A context contains a list of binders that “connects” the outer and inner worlds: these binders are carried by the constructors $\chi$.

A context and a term can be paired to produce a term-in-context:

\[
\begin{align*}
\text{CTm} & : \text{World} \rightarrow \text{Set} \\
\text{CTm} & = \exists[\beta](C^\alpha \beta \times Tm^\beta)
\end{align*}
\]
3.4. ADVANCED EXAMPLE: NORMALIZATION BY EVALUATION

It is straightforward to define a function \texttt{plug} from \( \text{CTm} \ \alpha \) to \( \text{Tm} \ \alpha \), which accepts a pair of a context and a term and plugs the latter into the former. Conversely, one can define a family of focusing functions \( (\forall \{\alpha\} \rightarrow \text{Tm} \ \alpha \rightarrow \text{CTm} \ \alpha) \), which split a term into a pair of a context and a term. There are several such functions, according to where one wishes to focus.

3.3.2 Patterns a la ML

As another instance of this idea, if one wished to extend our object language with ML-style patterns, one would index the type \texttt{Pat} of patterns with an outer world and an inner world, and one would use elaborate abstractions of the form \( \exists[\ \beta \ ](\text{Pat} \ \alpha \ \beta \times \text{Tm} \ \beta) \).

3.3.3 Term and types: System \( F \)

We use Girard-Reynold’s System \( F \) as an object language to illustrate how representations of object-level types can be indexed by worlds as well. Object-level terms are now indexed by two worlds: one for type names and one for term names.

```haskell
module SysF where

infixr 5 \_ ⇒_

data Ty α : Set where
  \_ ⇒_ : (x : Name α) → Ty α
  \_⇒_ : (σ τ : Ty α) → Ty α
  \‘∀‘ : ∀ b (τ : Ty (b < α)) → Ty α

data Tm α γ : Set where
  \_ : ∀ (x : Name α) → Tm α γ
  \_ : ∀ (t u : Tm α γ) → Tm α γ
  \_ : ∀ b (τ : Ty γ) (t : Tm (b < α) γ) → Tm α γ
  \_ : ∀ (τ : Tm α γ) (τ : Ty γ) → Tm α γ
  \_ : ∀ b (t : Tm α (b < γ)) → Tm α γ

Λ = ∀ b (t : Tm α (b < γ)) → Tm α γ

3.4 Advanced example: normalization by evaluation

As an advanced example, we show how to express a normalization by evaluation algorithm in our system. This algorithm has been previously used as a benchmark by several researchers [Shinwell et al., 2003, Pitts, 2006, Licata and Harper, 2009, Cave and Pientka, 2012]. The challenge lies in the way
the algorithm mixes computational functions, name abstractions, and fresh name generation.

The object language of interest is again the pure $\lambda$-calculus. The algorithm exploits two different representations of object-level terms, which are respectively known as *syntactic* and *semantic* representations. Because these representations differ only in their treatment of name abstractions, they can be given a common definition, which is parameterized over the representation of abstractions:

```agda
module M (Abs : (World → Set) → World → Set) where
data T α : Set where
  V : Name α  → T α
  ξ : Abs T α → T α
  ·· : T α → T α → T α

  The parameter Abs has kind (World → Set) → (World → Set): it is an indexed-type transformer.

  In order to obtain the syntactic representation, we instantiate Abs with the nominal abstractions that we have used everywhere so far: an abstraction is a package of a binder and of a term that inhabits the inner world. This yields the type Term of syntactic terms.

  SynAbsN : (World → Set) → World → Set
  SynAbsN F α = ∃[ b ](F (b ≪ α))

  open M SynAbs rename (T to Term)

  In order to obtain the semantic representation, we instantiate Abs with a different notion of abstraction, in the style of higher-order abstract syntax: an abstraction is a computational function, which substitutes a term for the bound name of the abstraction. This yields the type Sem of semantic terms. The type Sem is not an inductive data type; fortunately, with the --no-positivity-check flag, Agda accepts this type definition, at the cost of breaking strong normalization (to minimize the risks we isolated this kind of example to separate modules where this flag is activated).

  SemAbs : (World → Set) → World → Set
  SemAbs F α = ∀ {β} → α ⊆ β → F β → F β

  open M SemAbs rename (T to Sem)

  It is important to note that our semantic name abstractions involve bounded polymorphism in a world: we define SemAbs F α as ∀{β} → α ⊆ β → F β → F β, as opposed to the more naïve F α → F α. This
3.4. **ADVANCED EXAMPLE: NORMALIZATION BY EVALUATION**

provides a more accurate and more flexible description of the behavior of substitution. Indeed, when instantiating an abstraction $t$ with some term $u$, it makes perfect sense for $u$ to inhabit a larger world than $t$, that is, for $u$ to refer to certain names that are fresh for $t$. The result of the substitution then inhabits the same world as $u$: that is, it potentially refers to these fresh names, in addition to all of the names that occurred free in the abstraction $t$.

The types $\text{SemAbs}$ (and $\text{Sem}$), are covariant with respect to the parameter $\alpha$, which would not be the case with the naïve definition. In other words, it is possible to define a coerce operation for semantic terms:

$$
\text{coerceSem} : \forall \{\alpha \beta\} \to \alpha \sqsubseteq \beta \to \text{Sem} \alpha \to \text{Sem} \beta
$$

$$
\text{coerceSem} \, pf \, (V \, a) = V \, (\text{coerce}^\alpha pf \, a)
$$

$$
\text{coerceSem} \, pf \, (\lambda \, f \, v) = \lambda (\lambda \, pf' \, v \to f \, (\subseteq\text{-trans} \, pf \, pf') \, v)
$$

$$
\text{coerceSem} \, pf \, (t \cdot u) = \text{coerceSem} \, pf \, t \cdot \text{coerceSem} \, pf \, u
$$

At a semantic abstraction, no recursive call is performed, because the body of the abstraction is opaque: it is a computational function. Instead, we exploit the transitivity of world inclusion and build a new semantic abstraction that inhabits the desired world.

The normalization by evaluation algorithm makes use of environments. Here, environments are functions from names to semantic terms. The function $_,_,_\rightarrow$ shows how to extend such an environment:

$$
\text{EvalEnv} : (\alpha \beta : \text{World}) \to \text{Set}
$$

$$
\text{EvalEnv} \, \alpha \beta = \text{Name} \, \alpha \to \text{Sem} \, \beta
$$

$$
-\alpha \text{ is the inner world}
$$

$$
-\beta \text{ is the outer world}
$$

$$
_,_,_\rightarrow : \forall \{\alpha \beta\} \left(\Gamma : \text{EvalEnv} \, \alpha \beta\right) \, b \to \text{Sem} \, \beta \to \text{EvalEnv} \, (b \sqsubseteq \alpha) \, \beta
$$

$$
\text{- meaning: } b \mapsto v
$$

$$
\text{- } x \mapsto \Gamma \, x
$$

To a name, of type $\text{Name} \, \alpha$ an environment, of type $\text{EvalEnv} \, \alpha \beta$ associates a semantic term that lies outside the scope of the environment that is, a semantic term of type $\text{Sem} \, \beta$. The type $\text{EvalEnv} \, \alpha \beta$ is, again, covariant in its second world, as witnessed by the following coercion function:

$$
\text{coerceEnv} : \forall \{\alpha_1 \beta_1 \beta_2\} \to \beta_1 \sqsubseteq \beta_2 \to \text{EvalEnv} \, \alpha \beta_1 \to \text{EvalEnv} \, \alpha \beta_2
$$

$$
\text{coerceEnv} \, pf \, \Gamma = \text{coerceSem} \, pf \circ \Gamma
$$

The first part of the normalization by evaluation algorithm is a function $\text{eval}$ that evaluates a syntactic term within an environment to produce a semantic term. When evaluating a $\lambda$-abstraction, we build a semantic ab-
Stratification, which encapsulates a recursive call to `eval`. The bounded polymorphism required by the definition of semantic abstractions forces us to coerce the environment \( \Gamma \) via `coerceEnv`.

\[
\text{eval} : \forall \{\alpha \beta\} \rightarrow \text{EvalEnv} \alpha \beta \rightarrow \text{Term} \alpha \rightarrow \text{Sem} \beta
\]

\[
\text{eval} \; \Gamma \; (\chi \; (a \; t)) = \chi (\lambda \; pf \; v \rightarrow \text{eval} (\text{coerceEnv} \; pf \; \Gamma, \; a \mapsto v) \; t)
\]

\[
\text{eval} \; \Gamma \; (t \; u) = \text{app} (\text{eval} \; \Gamma \; t) (\text{eval} \; \Gamma \; u) \text{ where}
\]

\[
\text{app} : \forall \{\alpha\} \rightarrow \text{Sem} \alpha \rightarrow \text{Sem} \alpha \rightarrow \text{Sem} \alpha
\]

\[
\text{app} (\chi \; f) \; v = f \subseteq \text{refl} \; v
\]

\[
\text{app} \; n \; v = n \cdot v
\]

The second part of the algorithm reifies a semantic term back into a syntactic term. When reifying a semantic abstraction, we build a syntactic abstraction. This requires generating a fresh name, and leads us to parameterizing `reify` with a supply of fresh names.

\[
\text{reify} : \forall \{\alpha\} \rightarrow \text{Supply} \alpha \rightarrow \text{Sem} \alpha \rightarrow \text{Term} \alpha
\]

\[
\text{reify} \; s \; (V \; a) = V \; a
\]

\[
\text{reify} \; s \; (n \cdot v) = \text{reify} \; s \; n \cdot \text{reify} \; s \; v
\]

\[
\text{reify} (s^B, \; s^#) (\chi \; f) = \\
\chi (s^B, \; \text{reify} (\text{suc}^s (s^B, \; s^#)) (f (\subseteq \cdot s^#) (V (\text{name}^B \; s^B))))
\]

The constructor \( V \) has type `Name \alpha \rightarrow \text{Sem} \alpha` hence is a valid initial environment of type `EvalEnv \alpha \alpha`. Evaluation under this initial environment, followed with reification, yields a normalization algorithm. This algorithm works with open terms: its argument, as well as its result, are terms in an arbitrary world \( \alpha \). However this function needs a name supply for the world \( \alpha \). The name supply can be incrementally constructed with `zero^s` and `suc^s`. In particular we can normalize closed terms by giving `zero^s`:

\[
\text{nf} : \forall \{\alpha\} \rightarrow \text{Supply} \alpha \rightarrow \text{Term} \alpha \rightarrow \text{Term} \alpha
\]

\[
\text{nf} \; \text{supply} = \text{reify} \; \text{supply} \circ \text{eval} \; V
\]

Here is an example of the normalization of a term:

\[
\text{id}^T : \text{Term} \; \emptyset
\]

\[
\text{id}^T = \chi (0^B, \; V \; (0^s))
\]

\[
\text{test-nf} : \text{nf} \; \text{zero}^s ((\text{id}^T \cdot (\text{id}^T \cdot \text{id}^T)) \cdot \text{id}^T) \equiv \text{id}^T
\]

\[
\text{test-nf} = \text{refl}
\]
Chapter 4

Behind the scene of the NomPa library

4.1 Implementation of NomPa

The implementation of our interface is not surprising. Most of the code is types or proofs. Notice that this section details the internals of our library and that none of these definitions are meant to be known or used by the library client.

Worlds come first and are represented by lists of booleans. Such a list means that n is in the world if and only if the \( n^{th} \) value of the list is true. Formally the meaning of a world is defined by the membership predicate below. The choice of a list of booleans to represent a world was guided by two facts. First, the operations are structural: this eases the type-level computation and the proof goes through in particular in combination with de Bruijn indices as we details in section 5.2. Second, the elements are kept in order and (modulo trailing occurrences of false) two equivalent sets are represented the same way.

\[
\begin{align*}
\text{World} &: \text{Set} \\
\text{World} &= \text{List Bool} \\
\emptyset &: \text{World} \\
\emptyset &= [] \\
_\in_ &: \mathbb{N} \to \text{World} \to \text{Set} \\
_\in_ &= [\bot] \\
\text{zero} &\in (\text{false} :: _) = \bot \\
\text{zero} &\in (\text{true} :: _) = \top \\
\text{suc n} &\in (_ :: \text{xs}) = n \in \text{xs}
\end{align*}
\]
Worlds are meant to be computationally irrelevant. Meaning that none of the functions of this implementation make use of the worlds to compute the results. Hence, programs have an equivalent dynamic semantics when worlds are erased. While worlds are indeed used in membership, inclusion, and fresh-for proofs, these proofs are meant to be erased as well. Finally we want this erasing for three reasons: first for performances in the context of an optimizing compiler, second to have a separation between the “type system” and the running program, third to gain interesting theorems for free through the parametricity of world polymorphic functions (section 4.2).

Then binders are represented by natural numbers. The operator \( \_\triangleleft \_ \) defines how to extend a world with a binder. Given a binder \( n \) and a world \( \alpha \), \( n \triangleleft \alpha \) updates the world \( \alpha \) with the value true at index \( n \).

\[
\begin{align*}
\text{Binder} & : \text{Set} \\
\text{Binder} & = \mathbb{N} \\
\text{zero}^\text{Binder} & : \text{Binder} \\
\text{zero}^\text{Binder} & = \text{zero} \\
\text{suc}^\text{Binder} & : \text{Binder} \to \text{Binder} \\
\text{suc}^\text{Binder} & = \text{suc} \\
\_\triangleleft\_ & : \text{Binder} \to \text{World} \to \text{World} \\
\text{zero} \triangleleft [\] & = \text{true} :: [] \\
\text{suc} \ n \triangleleft [\] & = \text{false} :: \text{n} \triangleleft [] \\
\text{zero} \triangleleft (\_ :: \alpha) & = \text{true} :: \alpha \\
\text{suc} \ n \triangleleft (b :: \alpha) & = b :: \text{n} \triangleleft \alpha \\
\text{infixr} 5 \_\triangleleft\_ \\
\end{align*}
\]

The semantics of \( (y \triangleleft \alpha) \) is to add \( y \) to the set \( \alpha \). Precisely the semantics is described by the following lemma:

\[
\triangleleft\text{-sem} : \forall \alpha \ x \ y \to (x \in y \triangleleft \alpha) \equiv (\text{if } x \equiv \mathbb{N} \text{ then } \top \text{ else } x \in \alpha)
\]

Names are simply represented by a pair of a binder (a number) and a proof that this binder belongs to the indexing world. In \texttt{Agda} we use a record:
4.1. IMPLEMENTATION OF NOMPA

record Name α : Set where
  constructor _ -
  field
    binderN : Binder
    b ∈ α : binderN ∈ α
infixr 4 _ -
open Name public

To produce a name, \( \text{name}^B \) simply packs the given binder and a proof which is always constructible in this simple case:

\[
\text{name}^B : \forall \{\alpha\} \ b \to \text{Name} \ (b \triangleleft \alpha)
\]

\[
\text{name}^B \ b = b , \{! \text{proof omitted}!\}
\]

The equality test \( \text{==}_N \) and the exporting function \( \text{export}^N? \) both simply compare the internal representation of names and binders.

\[
\text{==}_N : \forall \{\alpha\} \ (x \ y : \text{Name} \ \alpha) \to \text{Bool}
\]

\[
\text{==}_N \ (x , _) \ (y , _) = x \text{==}N \ y
\]

\[
\text{export}^N? : \forall \{b \ \alpha\} \to \text{Name} \ (b \triangleleft \alpha) \to\ ? \text{Name} \ \alpha
\]

\[
\text{export}^N? \ {b} \ {\alpha} \ (x , \text{pf}) =
\]

\[
\text{if} \ x \text{==}N \ b \ \text{then} \ \text{nothing}
\]

\[
\text{else just} \ (x , \{! \text{proof omitted}!\})
\]

World inclusion is modeled as set-theoretic inclusion (membership preservation). This membership preservation proof is used by \( \text{coerce}^N \) to build the expected proof. All the inclusion rules (see figure 2.1) are computationally irrelevant and their implementations are omitted here.

\[
\infix 2 \subseteq
\]

\[
\subseteq : (\alpha \ \beta : \text{World}) \to \text{Set}
\]

\[
\alpha \subseteq \beta = \forall x \to x \in \alpha \to x \in \beta
\]

\[
\text{coerce}^N : \forall \{\alpha \ \beta\} \to \alpha \subseteq \beta \to \text{Name} \ \alpha \to \text{Name} \ \beta
\]

\[
\text{coerce}^N \ {\alpha} \subseteq \beta \ (b , \ \text{b} \in \alpha) = b \ , \ \alpha \subseteq \beta \ b \in \alpha
\]

The remaining part is the fresh-for relation (\( \# \)). To cope with the proof of \( \text{suc}^# \), we give two characterizations of this relation. One is a set of syntactic rules (omitted here) and the other is semantic. These presentations are equivalent [Pouillard, 2011a]. For pragmatic reasons the fresh-for relation is stronger than the non-membership relation (that is, \( x \# \alpha \) implies \( x \notin \alpha \) but the converse is false). The definition requires binder the be strictly greater that any binder in the world. This allows to build the \( \text{suc}^# \)
primitive rule (omitted here) without inspecting the world. Not inspecting the worlds at run-time is necessary since we want to erase worlds.

\[\_\_\_ : \text{Binder} \rightarrow \text{World} \rightarrow \text{Set}\]

\[x \# \alpha = \forall y (y \in \alpha \rightarrow x > y)\]

4.2 Soundness: logical relations and parametricity

Since our library is written in a type-safe language, one may wonder what soundness properties are to be proved. Moreover our names are indexed by worlds and hold membership proofs. The functions over names are given precise types and have been shown to be type-safe. The property that “well-typed programs do not go wrong” comes for free, but does not satisfy us. Indeed we have explained that certain operations (such as comparing two binders) must not be provided to programmers; the logical relation explains why this is the case.

To show that our library respects a model of good behavior with respect to names and binders, we build a model based on logical relations indexed/directed by types. This technique [Bernardy et al., 2010] is independent of this work and enables to define a notion of program equivalence. We use this technique to capture good behavior of functions involving names and binders. Using this technique, the set of specific definitions is kept to a minimum of one per introduced type (\text{World}, \text{Name}, and \_\subseteq\_). One proof per value introduced has to be done, which keeps the development modular and forward-compatible to the addition of more features.

This section is organized as follows. First we recall the basics of logical relations and parametricity. Then we give a toy example to practice a bit. Then relations for worlds, names, and world inclusions are given. Finally we make use of the construction to obtain free theorems [Wadler, 1989] about world-polymorphic functions over the type \text{Tm}.

4.2.1 Recap of the framework

A relation is said to be type-directed when it is recursively defined on the structure of types. Let \(\mathcal{R}\) be such a type-directed relation, and let \(\tau\) be a type. Then, \(\mathcal{R}_\tau\) is a relation on values of type \(\tau\), namely \(\mathcal{R}_\tau : \tau \rightarrow \tau \rightarrow \text{Set}\).

Recall that \text{Set} is also the type of propositions in \text{Agda}.

A type-directed relation is called “logical” when the case for functions is defined extensionally. Here “extensionally” means that two functions are related when they produce related results out of related arguments. Let \(A_r\) be a relation for the arguments and \(B_r\) a relation for results. Two functions \(f_1\) and \(f_2\) are related if and only if for every pair of arguments \((x_1, x_2)\) related
4.2. SOUNDNESS: LOGICAL RELATIONS AND PARAMETRICITY

by \( A_r \), the results \( f_1 \ x_1 \) and \( f_2 \ x_2 \) are related by \( B_r \). This definition can be given in Agda as well:

\[
\text{RelatedFunctions } A_r \ B_r \ f_1 \ f_2 = \\
\forall \{ x_1 \ x_2 \} \rightarrow A_r \ x_1 \ x_2 \\
\rightarrow B_r \ (f_1 \ x_1) \ (f_2 \ x_2)
\]

We say that a program or a value fits a logical relation when it is related to itself by the relation indexed by its type. We say that a logical relation is universal if every well-typed program fits the logical relation. This notion of universality was originally coined by John Reynolds as the “Abstraction Theorem” [Reynolds, 1983]. We call the “Agda logical relation” the one defined by Bernardy et al. [2010] for a PTS (pure type system) and naturally extended as suggested to other features of Agda. While no complete mechanized proof has been done for this we consider the Agda logical relation as universal.

To simplify matters, the definitions shown here are not universe-polymorphic. The reader can find universe-polymorphic definitions in our complete Agda development [Pouillard, 2011a].

To formally define a logical relation indexed by types, a common technique is to first inductively define the structure of types. This is known as a “universe of codes” \( U \). Then one defines a function called \( \text{El} \) from codes to types. Finally one defines by induction a function called \( \llbracket \_. \rrbracket \) from codes to relations on elements of type described by the given code. In Agda the function \( \llbracket \_. \rrbracket \) has the following type: \( (\tau : U) \rightarrow \text{El} \ \tau \rightarrow \text{El} \ \tau \rightarrow \text{Set} \). Because of quantification and dependent-types, types contain variables, and a good deal of complexity is added to this scheme, so we opt for a lighter scheme. We do not define \( U \), \( \text{El} \), and \( \llbracket \_. \rrbracket \).

Instead, for each type constructor \( \kappa \), we define a relation \( \llbracket \kappa \rrbracket \) (this is the name of the relation, since there are no spaces). For the function type constructor the \text{RelatedFunctions} definition above is a good start. Actually this is a fine definition for non-dependent functions. The dependent version of \text{RelatedFunctions}, called \( \llbracket \Pi \rrbracket \) here, passes the relation argument \( A_r \ x_1 \ x_2 \) called \( x_\rightarrow \) to the relation for results \( B_r \). In short the relation for results now depends on the relation for arguments. Here is the definition in Agda:

\[
\llbracket \Pi \rrbracket \ A_r \ B_r \ f_1 \ f_2 = \forall \{ x_1 \ x_2 \} \ (x_\rightarrow : A_r \ x_1 \ x_2) \\
\rightarrow B_r \ x_\rightarrow \ (f_1 \ x_1) \ (f_2 \ x_2)
\]

Note that this definition generalizes the case of non-dependent functions and universal quantifications as well. For non-dependent functions we simply provide a relation for results which ignores its first argument (equivalent to \text{RelatedFunctions} and noted \( _\llbracket \rightarrow \rrbracket \) from now on). For universal quan-
notifications, since the arguments are types, all we need is a relation for types (members of $\text{Set}_0$) themselves. Following our convention we call this relation $\llbracket \text{Set}_0 \rrbracket$. The relation $\llbracket \text{Set}_0 \rrbracket A_1 A_2$ is the set of relations between $A_1$ and $A_2$:

$$\llbracket \text{Set}_0 \rrbracket : \text{Set}_0 \to \text{Set}_0 \to \text{Set}_1$$

$$\llbracket \text{Set}_0 \rrbracket A_1 A_2 = A_1 \to A_2 \to \text{Set}_0$$

For reference, full definitions for core type theory are given in figure 4.1. As we said, we do not define the function $\llbracket \tau \rrbracket$. However we want a notation close to what this function would provide. To this end, instead of writing $\llbracket \tau \rrbracket$ for a given type expression $\tau$, we write $\tau$ where we replaced each constructor $\kappa$ by $\llbracket \kappa \rrbracket$, each non dependent arrow by $\llbracket \to \rrbracket$, each dependent arrow $(x : A) \to B$ by $\llbracket x_r : \llbracket A \rrbracket \rrbracket \to B$. By convention we subscript the names by $r$. Applications are translated to applications. Because of dependent types, this translation has to be extended to all terms but we do not do it here. Finally here are a few examples of the manual use of the function $\llbracket \cdot \rrbracket$:

```
-- What we would like to write but cannot:
[ N \to N \to \text{Bool} ] =

-- What we write instead:
[ N ] [ \to ] [ N ] [ \to ] [ \text{Bool} ] =

-- What this means:
\lambda f_1 f_2 \to
\forall \{ x_1 x_2 \} (x_r : [ N ] x_1 x_2)
\forall \{ y_1 y_2 \} (y_r : [ N ] y_1 y_2)
\to [ \text{Bool} ] (f_1 x_1 y_1) (f_2 x_2 y_2)

[ (A : \text{Set}_0) \to A \to A ] =
\llbracket \Pi \rrbracket \llbracket \text{Set}_0 \rrbracket (\lambda A_r A_r [ \to ] A_r) =
\lambda f_1 f_2 \to
\forall \{ A_1 A_2 \} (A_r : A_1 \to A_2 \to \text{Set}_0)
\forall \{ x_1 x_2 \} (x_r : A_r x_1 x_2)
\to A_r (f_1 A_1 x_1) (f_2 A_2 x_2)

-- Using the notation instead of $\llbracket \Pi \rrbracket$:
[ A : \text{Set}_0 ] \to \text{List} A ] =
\langle A_r : [ \text{Set}_0 ] \to [ \text{List} ] A_r \rangle =
\lambda l_1 l_2 \to
\forall \{ A_1 A_2 \} (A_r : A_1 \to A_2 \to \text{Set}_0)
\to [ \text{List} ] A_r (l_1 A_1) (l_2 A_2)
```

We now have the definition of the AGDA logical relation for the core
4.2. **SOUNDNESS: LOGICAL RELATIONS AND PARAMETRICITY**

\[
\begin{align*}
\text{\([\text{Set}_0]\)} & : \forall (A_1 A_2 : \text{Set}_0) \rightarrow \text{Set}_1 \\
\text{\([\text{Set}_0]\)} & A_1 A_2 = A_1 \rightarrow A_2 \rightarrow \text{Set}_0 \\
\text{\([\text{Set}_1]\)} & : \forall (A_1 A_2 : \text{Set}_1) \rightarrow \text{Set}_2 \\
\text{\([\text{Set}_1]\)} & A_1 A_2 = A_1 \rightarrow A_2 \rightarrow \text{Set}_1 \\
\end{align*}
\]

- \([\rightarrow]\_ : \forall \{A_1 A_2 B_1 B_2\} \rightarrow \text{\([\text{Set}_0]\)} A_1 A_2 \rightarrow \text{\([\text{Set}_0]\)} B_1 B_2 \\
\quad \rightarrow \text{\([\text{Set}_1]\)} (A_1 \rightarrow B_1) (A_2 \rightarrow B_2) \\
A_r \ [\rightarrow]_\_ B_r = \lambda f_1 f_2 \rightarrow \forall \{x_1 x_2\} \rightarrow A_r x_1 x_2 \rightarrow B_r (f_1 x_1) (f_2 x_2)

\text{infixr 0 } _{\rightarrow}_-

\[\text{II} : \forall \{A_1 A_2\} (A_r : \text{\([\text{Set}_0]\)} A_1 A_2) \\
\quad \rightarrow \text{\([\text{Set}_0]\)} B_1 B_2 : (B_r : (A_r \ [\rightarrow]_\_ \text{\([\text{Set}_0]\)} A_1 A_2) \\
\quad \rightarrow (\{x : A_1\} \rightarrow B_1 x) \rightarrow (\{x : A_2\} \rightarrow B_2 x) \rightarrow \text{Set}_1 \\
\text{II} & A_r B_r = \lambda f_1 f_2 \rightarrow \forall \{x_1 x_2\} (x_r : A_r x_1 x_2) \rightarrow B_r x_r (f_1 x_1) (f_2 x_2)

\text{syntax } \text{II} A_r (\lambda x_r \rightarrow f) = \langle x_r : A_r \rangle [\rightarrow] f

\[\forall : \forall \{A_1 A_2\} (A_r : \text{\([\text{Set}_0]\)} A_1 A_2) \\
\quad \rightarrow \text{\([\text{Set}_0]\)} B_1 B_2 : (B_r : (\text{\([\text{Set}_0]\)} [\rightarrow] \text{\([\text{Set}_0]\)} A_1 A_2) \\
\quad \rightarrow \{x : A_1\} \rightarrow B_1 x) \rightarrow \{x : A_2\} \rightarrow B_2 x \\
\forall & A_r B_r = \lambda f_1 f_2 \rightarrow \forall \{x_1 x_2\} (x_r : A_r x_1 x_2) \rightarrow B_r x_r (f_1 x_1) (f_2 x_2)

\text{syntax } \forall A_r (\lambda x_r \rightarrow f) = \forall \{ x_r : A_r \} [\rightarrow] f

Figure 4.1: Logical relations for core types
type theory part. It extends nicely to inductive data types and records. The process is as follows: for each constructor $\kappa$ of type $\tau$, declare a new constructor $J_\kappa$ whose type is $J_{\tau} J_\kappa J_\kappa$. This process applies to type constructors and data constructors of data types, and type constructors and fields of record types. For reference, the logical relations for the data types we use in this development are in figure 4.2.

**Parametricity results: “Theorems For Free”** We have explained how Agda’s logical relation is defined ($J_{\tau} J$) on various types. We can now more precisely explain how to use the “Abstraction theorem” associated to Agda terms.

For every well-typed term $M$ at type $\tau$, the theorem $J_{\tau} M M$ is provable.

In Type Theory (such as Agda and Coq) the specification language is the same as the programming language, which helps a lot. The theorem statement: $J_{\tau} M M$ is a valid type in Agda and a proof of it is a term of this type.

We warmly recommend the reader to study [Bernardy et al., 2010] to get a more in-depth understanding on the subject. We still try to give some insight on the “Abstraction Theorem”. We write $\Gamma \vdash M : \tau$ for a typing judgement on Agda terms. In such a judgement, $\Gamma$ is a typing environment holding previously defined terms and data types. While we explained how $J_{\tau}$
4.2. SOUNDERNESS: LOGICAL RELATIONS AND PARAMETRICITY

is defined on types, it extends nicely on terms which is actually necessary in
Agda since terms and types cohabit. The meta-function $\llbracket \cdot \rrbracket$ is also defined
on environments by translating each binding of the environment.

$$\Gamma \vdash M : \tau \Rightarrow \llbracket \Gamma \rrbracket \vdash \llbracket M \rrbracket : \llbracket \tau \rrbracket M M$$

This theorem reads like, for all term $M$, well-typed under environment $\Gamma$
at type $\tau$, the term $\llbracket M \rrbracket$ is well-typed under environment $\llbracket \Gamma \rrbracket$ at type
$\llbracket \tau \rrbracket M M$. If we read the type $\llbracket \tau \rrbracket M M$ as a proposition then the term $\llbracket M \rrbracket$
is its proof.

Hence, every well-typed term give rise to a free-theorem thanks to para-
metricity. However interesting results arose only when using polymorphism.
In our setting polymorphism comes at two places. First, by making the
types of our interface abstract we force the client to be polymorphic with
respect to these types. Second, when the client write a world-polymorphic
function this give rise to even more powerful parametricity results. In sec-
tion 5.4.3 we give a more detailed account to various function types and
their respective strength.

4.2.2 An example: Boolean values represented by numbers

We wish to explain how logical relations can help explain in what sense
the interface to an abstract type is safe. To do so we introduce a tiny
example about booleans represented using natural numbers. We want 0
to represent $\text{false}$ and any other number to represent $\text{true}$. Therefore
the boolean disjunction can be implemented using addition. We show that
logical relations help build a model, ensure that a given implementation
respects this model, and finally show that a client that uses only the interface
also respect the model.

Note however that this is a toy example in several ways. There are no
polymorphic functions in the interface, so no interesting free theorems are
to be expected. While we could prove safety by defining a representation
predicate in unary style, the logical relations approach is different. It re-
lies on comparing concrete data as opposed to mapping to abstract data.
The unary style would allow for a simpler construction, however this over-
simplifies the problem here and would be no longer useful for proving our
library.

Our tiny implementation of booleans using natural numbers is given
below. It contains a type $B$ that we want to keep abstract. It contains
obvious definitions for $\text{true}, \text{false}$, and the disjunction $\lor$. It intentionally
has a dubious function $\text{is42?}$. Given that 42 and 41 both represent a truth
value, the function $\text{is42?}$ returns different results. This dubious function
breaks our still informal expectations from such a module.
\[ B : \text{Set} \]
\[ B = \mathbb{N} \]

\[ \text{false} : B \]
\[ \text{false} = 0 \]

\[ \text{true} : B \]
\[ \text{true} = 1 \]

\[ \text{\_} \lor \text{\_} : B \rightarrow B \rightarrow B \]
\[ m \lor n = m + n \]

\[ \text{is42?} : B \rightarrow B \]
\[ \text{is42?} 42 = \text{true} \]
\[ \text{is42?} \_ = \text{false} \]

The next step is to define our expectations. To do so, we give a binary relation which tells when two \( B \) values have the same meaning. We do so with an (inductive) data type named \([B] \) which states that 0 is related only with itself, and that any two non zero numbers are related, formalizing the intuition that two non zero numbers mean the same thing:

\[
data \; \text{[B]} : B \rightarrow B \rightarrow \text{Set} \; \text{where}
\text{[false]} : [B] \; 0 \; 0
\text{[true]} : \forall \{m \; n\} \rightarrow [B] \; (\text{suc} \; m) \; (\text{suc} \; n)
\]

When plugged into the machinery of logical relations this single definition suffices to define a complete model of well-typed programs. However, the plumbing requires some care. While the AGDA logical relation is universal, we have no such guarantee about the AGDA logical relation where the relation for \( B \) is no longer \([\mathbb{N}] \) but \([B] \). Fortunately changing the relation at a given type (\( B \) here) can be done safely. All we have to do is to consider programs abstracted away from \( B \) and its operations: \text{true, false} and \text{\_} \lor \text{\_. This can be done either through a mechanism for abstract types, or by requiring the client to be a function taking the implementation for \( B \) and its operations as argument.}

However, to use \([B] \) as the relation for \( B \), we have to show that the definitions which make use of the representation of \( B \) actually fit the relation. Since \([true]\) and \([false]\) are obvious witnesses for \text{true} and \text{false}, only \text{\_} \lor \text{\_} and \text{is42?} are left to be proved. Each time the goal to prove is systematic: wrap the type with \([\cdot]\) on each constructor and put the name of the function twice to state we want it to be related to itself. Here is the definition for \([\_] \lor \text{\_.} :\]
4.3 RELATIONS FOR NOMPA

_{\lor} : (\text{[B]} \rightarrow \text{[B]} \rightarrow \text{[B]}) \rightarrow \text{[B]}

The type of _{\lor} means that given inputs related in the model, the results are related in the model as well. Once unfolded the type looks like:

\[ \forall \{x_1, x_2\} (x_r: \text{[B]} x_1 x_2) \rightarrow \text{[B]} (x_1 \lor y_1) (x_2 \lor y_2) \]

The fact that input arguments come as implicit arguments greatly shortens definitions. Now, thanks to the inductive definition of _+_, pattern-matching on the first relation suffices to reduce the goal, and allows this nice-looking definition of _{\lor} where we see the usual lazy definition of the left biased disjunction:

false \lor x = x
true \lor _ = [true]

Let us now consider a proof for the function is42?. Fortunately there is no such proof since this function gladly breaks the intended abstraction. Instead we simply prove its negation by exhibiting that given two related inputs (42 and 27) we get non related outputs (since is42? 42 = 1 and is42? 27 = 0).

\[-is42? : \neg((\text{[B]} \rightarrow \text{[B]}) \text{is42? is42?})
\neg-is42? with [is42?] \{42\} \{27\} \text{[true]}
... | () \rightarrow absurd\]

Note that is42? is rejected by our model with no considerations about the other exported functions. Here we have a means to build 42 by using _\lor_ and true. However with another implementation of _\lor_ there would be no way to produce 42 and so no way to expose the wrong behavior of is42? using the interface. This would enable some proof techniques to actually show that no harm can be done given the limited interface and implementation. Such a proof would break down when extending the interface. In the end, using a model provides a better forward compatibility than syntactic proof techniques and enables proofs to be done in a modular way.

4.3 Relations for NomPa

For NomPa, we apply the same process as with booleans. We define our expectations, by defining relations for introduced abstract types (worlds, binders, names, fresh-for and inclusions). Finally we prove that each value
and/or function exported fits the relation.

### 4.3.1 Relations for NomPa types

For reference the definitions are given in figure 4.3. We now describe them in turn.

While the types and the worlds define the programs we accept as valid, logical relations define when two programs have the same “meaning”. For instance, valid names are those which belong to their worlds, names with the same meaning are those related by the relation between their worlds. What matters is not just the fact that two worlds $\alpha_1$ and $\alpha_2$ are related, what matters is how they are related, because this dictates when a name in $\alpha_1$ and a name in $\alpha_2$ are related. Thus we define $\llbracket \text{World} \rrbracket \alpha_1 \alpha_2$ to be a set of relations between Name $\alpha_1$ and Name $\alpha_2$ (we note $\alpha_r$ a relation of type $\llbracket \text{World} \rrbracket \alpha_1 \alpha_2$).

Which relations should be part of this set? The more relations are part of it, the more power this gives to parametricity results... However, in order for the equality test on names to inhabit the logical relation, we must restrict $\llbracket \text{World} \rrbracket \alpha_1 \alpha_2$ to contain only relations that preserve equality in both directions, that is, only functional and injective relations:

\[
\text{Preserve-}\equiv \quad R = \\
\forall x_1 y_1 x_2 y_2 \rightarrow R \quad x_1 \equiv x_2 \rightarrow R \quad y_1 \equiv y_2 \\
\rightarrow x_1 \equiv y_1 \leftrightarrow x_2 \equiv y_2
\]

The relation $\llbracket \text{Name} \rrbracket$ is parameterized by a relation over worlds. Given two worlds $\alpha_1$ and $\alpha_2$, and a relation $\alpha_r$ between them (the world $\alpha_r$ has type $\llbracket \text{World} \rrbracket \alpha_1 \alpha_2$), then a name $x_1$ in $\alpha_1$ is related to a name $x_2$ in $\alpha_2$ if and only if they are related by $\alpha_r$: $\alpha_r \ x_1 \ x_2$. In short, the relation between names is completely defined by the relation between their worlds.

The relation $\llbracket \text{Binder} \rrbracket$ between two binders is both simple and meaningful. It is simple since it is the full relation, meaning that any two binders are related by $\llbracket \text{Binder} \rrbracket$. It is meaningful since it recalls us that one binder is not better than another one. For instance when comparing object-level terms as we do in section 3.1.3, the functions $\text{cmpTm}$ and $\text{==Tm}$ never compare binders.

This definition is meaningful for a second reason that appears when one looks at the free-theorems associated with functions that expect binders. For instance, a well-typed function $f$ of type $\text{Binder} \rightarrow \text{Binder} \rightarrow \text{Bool}$ can only be a constant function!
4.3. RELATIONS FOR NOMPA

-- \([f]\) is the parametricity theorem of \(f\)
\[\begin{array}{l}
[f] : ([\text{Binder}] \to [\text{Binder}] \to [\text{Bool}]) f f
\end{array}\]

-- \(f\)-const is a corollary of \([f]\).
-- \(f\)-const shows that \(f\) is a constant function.
\[f\text{-const} : \forall x_1 x_2 y_1 y_2 \to f x_1 y_1 \equiv f x_2 y_2\]
\[f\text{-const} x_1 x_2 y_1 y_2\text{ with }[f] \{x_1\} \{x_2\} \to \{y_1\} \{y_2\} \to \]
\[\ldots \mid [\text{true}] = \text{refl}\]
\[\ldots \mid [\text{false}] = \text{refl}\]

This proves that there must be no way to distinguish two binders!

For the \(_{\subseteq}\)_ relation, we exploit the fact there is only one way to use an inclusion witness, namely \(\text{coerce}^N\). Thus, for the purpose of building the “model”, we identify inclusions with their use in \(\text{coerce}^N\). That is, two witnesses \(\alpha_1 \subseteq \beta_1\) and \(\alpha_2 \subseteq \beta_2\) are related if and only if \(\text{coerce}^N\alpha_1 \subseteq \beta_1\) and \(\text{coerce}^N\alpha_2 \subseteq \beta_2\) are related (see figure 4.3). Another way to look at it is from the perspective of relation inclusion. A relation \(R_1\) is included in a relation \(R_2\) if and only if all pairs related by \(R_1\) are related by \(R_2\) as well.

Because the function \(\text{coerce}^N\) behaves such as the identity function, these two definitions coincide. If we expand the definitions for \([\text{Name}]\) and \(\vdash \to \vdash\), we find that \(\alpha_1 \subseteq \beta_1\) and \(\alpha_2 \subseteq \beta_2\) are related if and only if the relation \(\alpha_r\) is included in the relation \(\beta_r\):

\[\begin{array}{l}
_{\subseteq} \alpha_r \beta_r \alpha_1 \subseteq \beta_1 \alpha_2 \subseteq \beta_2
\quad = \forall \{x_1 x_2\} \to (x_1, x_2) \in \alpha_r
\quad \to (\text{coerce}^N\alpha_1 \subseteq \beta_1 x_1, \text{coerce}^N\alpha_2 \subseteq \beta_2 x_2) \in \beta_r
\end{array}\]

We now have to define operations on worlds that fit the logical relation.

The case for \([\emptyset]\) is trivial and uniquely defined. There is only one relation between empty sets: the empty relation.

\[\emptyset : [\text{World}] \emptyset \emptyset\]

We give below a set-theoretic definition of \(\_\ll\_\). Our definition is not based on sets but equivalent to this. This new relation is shown to preserve the equalities.

\[\begin{array}{l}
\ll : ([\text{Binder}] \to [\text{World}] \to [\text{World}] \to [\text{World}]) \ll \ll \ll
\quad \text{-- not proper Agda}
\end{array}\]

\[\begin{array}{l}
b_r \ll \alpha_r \overset{\text{def}}{=} \{ (b_1, b_2) \} \cup \{ (x, y) \mid (x, y) \in \alpha_r \land x \neq b_1 \land y \neq b_2 \}
\end{array}\]
Figure 4.3: Relations for NomPa types
4.3. RELATIONS FOR NOMPA

Here is a small drawing of the effect of $\llbracket \varphi \rrbracket$ on relations between names:

4.3.2 NomPa values fit the relation

We now give a short overview of the proofs needed to show that our functions fit the relation. Formally, for each primitive operation $p$ which has type $\tau$ in our interface, we have to exhibit a definition $\llbracket p \rrbracket$ which has type $\llbracket \tau \rrbracket p p$. All the proof can be found in our Agda development [Pouillard, 2011a]. Thanks to the definition of $\llbracket \text{Binder} \rrbracket$, $\text{zero}^B$ and $\text{suc}^B$, any function that returns a binder immediately fit the relation. The same reasoning holds for $\llbracket \emptyset \rrbracket$ and $\text{suc}^\emptyset$ that immediately fit the relation. Thanks to the definition of $\llbracket \llbracket \varphi \rrbracket \rrbracket$, $\llbracket \text{name}^B \rrbracket$ holds by definition. Since $\llbracket \lnot \text{Name} \rrbracket$ receives names in the empty world, it trivially holds. For instance here is the type signature for $\llbracket \text{name}^B \rrbracket$:

\[
\llbracket \text{name}^B \rrbracket : (\forall \{ \alpha_1 \alpha_2 \} (\alpha_r : \llbracket \text{World} \rrbracket \alpha_1 \alpha_2) \\
( b_r : \llbracket \text{Binder} \rrbracket b_1 b_2) \\
\llbracket \text{Name} \rrbracket ( b_r \llbracket \llbracket \varphi \rrbracket \alpha_r ) \\
) \text{name}^B \text{name}^B
\]

$\llbracket \llbracket \text{==} \rrbracket \rrbracket$, once unfolded, the statement tells that the equality test commutes with a renaming. This means that the result of the equality test does not change when its inputs are consistently renamed. The proof for $\llbracket \llbracket \text{==} \rrbracket \rrbracket$ is done in two parts. First, we have to relate the boolean valued function $\llbracket \text{==} \rrbracket$ to the fact it decides equality on names. Second, we make full use of the equality preservation property.
CHAPTER 4. BEHIND THE SCENE OF THE NOMPA LIBRARY

\[
\begin{align*}
&\forall \langle \alpha_r : \text{World} \rangle \rightarrow \text{Name} \\
&\forall \langle \alpha_r : \text{World} \rangle \rightarrow \text{Name} \\
&\forall \langle \alpha_r : \text{World} \rangle \rightarrow \text{Name} \\
&\forall \langle \text{Bool} \rangle \rightarrow \text{bool} \\
&\forall \langle \alpha_1 \alpha_2 \rangle \rightarrow \alpha_1 \alpha_2 \\
&\forall \langle \alpha_1 \alpha_2 \rangle \rightarrow \alpha_1 \alpha_2 \\
&\forall \langle \text{Bool} \rangle \rightarrow \text{bool} \\
&\forall \langle \alpha_1 \alpha_2 \rangle \rightarrow \alpha_1 \alpha_2 \\
&\forall \langle \alpha_1 \alpha_2 \rangle \rightarrow \alpha_1 \alpha_2 \\
\end{align*}
\]

The proof that \text{export}^N is in the relation relies on two points. First, the success (returning \text{just} or \text{nothing}) of \text{export}^N \{b\} \cdot x depends only on the equality between (\text{name}^N b) and x. Second, the worlds related by (b \sqsubseteq^N \alpha_r) can always be split into two groups, those being related by (b \sqsubseteq^N \emptyset) and those related by \alpha_r. Said differently there is no link between the two parts.

Thanks to the definition of \(\subseteq^N\), the proof that \text{coerce}^N fits the relation is a simple application of the hypotheses. Then the real job is to show that all the inclusion rules fit the relation. This means that they all behave as the identity function. In the end all the logical relation proofs associated with all our primitive operations and rules are formally proved in our Agda development [Pouillard, 2011a].

4.3.3 An example not fitting the relation

For instance consider the introduction of this function to compare two names:

\[
\begin{align*}
\forall \langle \alpha \rangle &\rightarrow \text{Name} \\
\forall \langle \alpha \rangle &\rightarrow \text{Name} \\
\forall \langle \alpha \rangle &\rightarrow \text{Name} \\
\forall \langle \text{Bool} \rangle &\rightarrow \text{bool} \\
\forall \langle \alpha_1 \alpha_2 \rangle &\rightarrow \alpha_1 \alpha_2 \\
\forall \langle \alpha_1 \alpha_2 \rangle &\rightarrow \alpha_1 \alpha_2 \\
\forall \langle \text{Bool} \rangle &\rightarrow \text{bool} \\
\forall \langle \alpha_1 \alpha_2 \rangle &\rightarrow \alpha_1 \alpha_2 \\
\forall \langle \alpha_1 \alpha_2 \rangle &\rightarrow \alpha_1 \alpha_2 \\
\end{align*}
\]

This function is accepted by Agda type-checking rules but does not meet our property that well-behaved functions should map \(\alpha\)-equivalent inputs to \(\alpha\)-equivalent outputs.

\[
\begin{align*}
\forall \langle \text{Bool} \rangle &\rightarrow \text{bool} \\
\forall \langle \alpha_1 \alpha_2 \rangle &\rightarrow \alpha_1 \alpha_2 \\
\forall \langle \text{Bool} \rangle &\rightarrow \text{bool} \\
\forall \langle \alpha_1 \alpha_2 \rangle &\rightarrow \alpha_1 \alpha_2 \\
\forall \langle \alpha_1 \alpha_2 \rangle &\rightarrow \alpha_1 \alpha_2 \\
\forall \langle \alpha_1 \alpha_2 \rangle &\rightarrow \alpha_1 \alpha_2 \\
\forall \langle \text{Bool} \rangle &\rightarrow \text{bool} \\
\forall \langle \alpha_1 \alpha_2 \rangle &\rightarrow \alpha_1 \alpha_2 \\
\forall \langle \alpha_1 \alpha_2 \rangle &\rightarrow \alpha_1 \alpha_2 \\
\end{align*}
\]

-- parts ('?') of the proofs are omitted for conciseness
Chapter 5

The de Bruijn approach

So far, we only considered a nominal representation. This is not the only way to deal with names and binders. We now focus on a different kind of representation, namely de Bruijn indices [de Bruijn, 1972]. This representation is said to be nameless because binders are no longer identified by an atom but by a notion of “distance” to the binding point.

This nameless approach solves part of the problem of representing binders by providing a canonical representation. More precisely binding occurrences are no longer named (we now use \(\lambda\), instead of \(\lambda x.\)). Bound variables are represented by the “distance” to the binding \(\lambda\). This distance is the number (starting from 0) of enclosing \(\lambda\)s to cross in order to reach the binding \(\lambda\).

This approach to a safer way to program with de Bruijn indices is described in our previous paper called “Nameless, Painless” [Pouillard, 2011b]. The library specialized to de Bruijn indices is called NaPa for Nameless Painless. However we here stick to the general approach.

This chapter is organized as follows. The first section introduces de Bruijn indices through successive variations found in the literature. The second section 5.2, extends our programming interface in order to support de Bruijn indices. Also, the implementation is extended and not replaced. Section 5.3 explains how to use the interface to write functions on a de Bruijn representation of programs. In section 5.4 we extend the logical relation to support the de Bruijn style and we show how to exploit these properties on concrete examples.

5.1 Introduction to de Bruijn indices

Various techniques have been discovered to build a nameless representation. We have chosen a few of them which gradually set up the stage.
5.1.1 bare: The original approach

We call this one bare, because it relies solely on natural numbers. To make things more concrete here is an example of its use when defining our usual type for terms:

```haskell
data Tm^B : Set where
  V : (x : N) → Tm^B
  _·_ : (t u : Tm^B) → Tm^B
  X : (t : Tm^B) → Tm^B
  Let : (t u : Tm^B) → Tm^B
```

From the point of view of the binding structure, it is striking that no difference appears between the constructors of the data type. It is completely up to the programmer to manage the scoping difference introduced by \( X \) and \( \text{Let} \). This is even more worrying in the \( \text{Let} \) case since we have no clue of difference between the arguments.

Here is an example using this representation to build the \( \lambda \)-term for function application, namely \( \lambda f.\lambda x.f\ x \).

```haskell
appTm^B : Tm^B
appTm^B = X (X (V 1 · V 0))
```

The main advantages of this approach are its simplicity and its expressiveness. The expressiveness is maximal since no restriction is put on the usage of variables.

5.1.2 Maybe: The nested data type approach

The nested data type approach [Bellegarde and Hook, 1994, Bird and Paterson, 1999, Altenkirch and Reus, 1999] is a first step towards better properties about the binding structure of terms. Let us start with the definition of our type for terms with this approach:

```haskell
data Tm^M (A : Set) : Set where
  V : (x : A) → Tm^M A
  _·_ : (t u : Tm^M A) → Tm^M A
  X : (t : Tm^M (Maybe A)) → Tm^M A
  Let : (t : Tm^M A) (u : Tm^M (Maybe A)) → Tm^M A
```

There are three points to look at. The type \( Tm^M \) is parameterized by another type called \( A \), so we can look at it as a kind of container. Note also that the variable case \( V \) does not hold a value of type \( N \) but a value of type \( A \). Last but not least the \( X \) case holds a term whose parameter is not
simply a value of type \( A \) but a value of type \( \text{Maybe } A \).

This last point makes the type \( \text{Tm}^n \) a nested data type, also called a non-regular type. This has the consequence of requiring polymorphic recursion to write recursive functions on such a type.

To understand why this is an adequate representation of \( \lambda \)-terms one has to look a bit more at the meaning of \( \text{Maybe} \). If types are seen as sets, then \( \text{Maybe} \) takes a set and returns a set with one extra element. So each time we cross a \( \lambda \), there is one extra element in the set of allowed variables, exactly capturing the fact that we are introducing a variable.

To see the difference with the previous approach, here is the \( \lambda \)-term for function application again:

\[
\text{appTm}^n : \text{Tm}^n \perp \\
\text{appTm}^n = \lambda (V \text{ (just nothing)} \cdot V \text{ nothing})
\]

Note the use of the empty type \( \perp \) to state the closedness of the \( \text{appTm}^n \) term. Stating this kind of properties was impossible to do with the previous approach, without resorting to logical properties on the side.

### 5.1.3 The \( \text{Fin} \) approach

Another approach already described and used in [Altenkirch, 1993, McBride and McKinna, 2004] is to index everything (terms for example) by a bound. This bound is the maximum number of distinct free variables allowed in the value. This rule is enforced in two parts: variables have to be strictly lower than their bound, and the bound is incremented by one when crossing a name abstraction (a \( \lambda \)-abstraction for instance, called \( \lambda \) here).

The type \( \text{Fin } n \) is used for variables and represents natural numbers strictly lower than \( n \). The name \( \text{Fin } n \) comes from the fact that it defines finite sets of size \( n \). We call this approach \( \text{Fin} \) for its use of this type. The definition found in Agda’s standard library is the following:

\[
data \text{Fin} : \mathbb{N} \to \text{Set} \text{ where}
\begin{align*}
\text{zero} & : \{n : \mathbb{N}\} \to \text{Fin} (\text{suc } n) \\
\text{suc} & : \{n : \mathbb{N}\} (i : \text{Fin } n) \to \text{Fin} (\text{suc } n)
\end{align*}
\]

Given this type \( \text{Fin} \), one can define the term data type using this approach:

\[
data \text{Tm}^f n : \text{Set} \text{ where}
\begin{align*}
\text{V} & : (x : \text{Fin } n) \to \text{Tm}^f n \\
\lambda \cdot \lambda & : (t \ u : \text{Tm}^f n) \to \text{Tm}^f n \\
\lambda & : (t : \text{Tm}^f (\text{suc } n)) \to \text{Tm}^f n \\
\text{Let} & : (t : \text{Tm}^f n) (u : \text{Tm}^f (\text{suc } n)) \to \text{Tm}^f n
\end{align*}
\]
As the previous approach, this representation helps enforce some well-formedness properties, for instance $\text{Tm}^f_0$ is the type of closed $\lambda$-terms.

Here is the $\lambda$-term for application in this approach:

$$\text{appTm}^f : \text{Tm}^f_0$$

$$\text{appTm}^f = \lambda (\lambda (V (\text{suc zero}) \cdot V \text{zero}))$$

We can easily draw a link with the Maybe approach. Indeed, the type $\text{Fin} (\text{suc } n)$ has exactly one more element than the type $\text{Fin } n$. However, these approaches are not equivalent for at least two reasons. The Maybe approach can accept any type to represent variables. This makes the structure more like a container and this can be particularly helpful to define the substitution as the composition of $\text{mapTm} : \forall \{A B\} \rightarrow (A \rightarrow B) \rightarrow \text{Tm } A \rightarrow \text{Tm } B$ and $\text{joinTm} : \forall \{A\} \rightarrow \text{Tm } (\text{Tm } A) \rightarrow \text{Tm } A$ as in [Bellegarde and Hook, 1994, Bird and Paterson, 1999, Altenkirch and Reus, 1999]. The Fin approach has advantages as well: the representation is concrete and simpler since closer to the bare approach. However this apparent simplicity comes at a cost: we will see that its concrete representation is one root of the problem.

### 5.2 An interface for de Bruijn indices

In order to effectively program with de Bruijn indices we wanted to have a dedicated programming interface. This is indeed in contrast with our previous work [Pouillard and Pottier, 2010] where we had two implementations – nominal and de Bruijn – of a common interface.

We now claim that we need specialized operations to better support nominal and de Bruijn styles. Happily the work done for nominal nicely scales to de Bruijn indices by adding new primitive operations on worlds, names, and world inclusions.

Following the development that we have done for the nominal representation, we index names and terms by worlds. Everything we have built so far remains valid (and useful). The types and definitions for $\text{World}$, $\emptyset$, $\text{Name}$, $\text{==}$, $\text{¬}$, $\subseteq$, $\text{coerce}$, $\subseteq\text{-refl}$, $\subseteq\text{-trans}$ and $\subseteq\emptyset$ are directly re-used.

While binders ($\text{Binder}$, $\text{◁}$, zero$B$, suc$B$...) do not need to be exposed in order to follow a de Bruijn presentation, we use them in the implementation of de Bruijn primitive operations.

To understand what definitions we need to add to deal with de Bruijn indices, we identify two characteristics of a binding construct such as $\lambda$. With de Bruijn indices two things occur at $\lambda$-abstractions: $0$ is introduced as a new binder, and all the previous binders are incremented by one.
The key feature of this approach is to change how binders are referenced in a particular subterm. Our explicit notion of world can be used to express this change. We extend our notion of worlds with an operator \( \_\_+1 \) (formally defined on page 98). Since worlds can be thought of as sets, the operator \( \_\_+1 \) has an informal set-theoretic definition of adding one to each element of the set. Postponing a formal definition, here is the declaration:

\[ \_\_+1 : \text{World} \rightarrow \text{World} \]

With this single extension of world operations \( \_\_+1 \), we can build name abstractions in the style of de Bruijn indices. Here is our type \( \text{Tm}^D \) revised to follow de Bruijn indices:

\[
\begin{align*}
\text{data } \text{Tm}^D \alpha : \text{Set} & \text{ where } \\
V & : \text{Name } \alpha \rightarrow \text{Tm}^D \alpha \\
\_\_ : \text{Tm}^D \alpha & \rightarrow \text{Tm}^D \alpha \rightarrow \text{Tm}^D \alpha \\
\check & : \text{Tm}^D (0 \_B \check{} (\alpha \_+1)) \rightarrow \text{Tm}^D \alpha \\
\text{Let} & : \text{Tm}^D \alpha \rightarrow \text{Tm}^D (0 \_B \check{} (\alpha \_+1)) \rightarrow \text{Tm}^D \alpha \\
\end{align*}
\]

The only change between \( \text{Tm} \) and \( \text{Tm}^D \) is in the binding constructs. Instead of holding a binder \( b \) that is bound in the subterm, \( 0 \_B \) is bound in the subterm and all the previous binders are moved by one. Because this world operation is idiomatic, it deserves its own notation:

\[ \_\_\uparrow1 : \text{World} \rightarrow \text{World} \]

\[ \alpha \_\_\uparrow1 = 0 \_B \check{} (\alpha \_+1) \]

We get back the nested data type approach described in section 5.1.2 if one replaces \( \text{World} \) by \( \text{Set} \), \( \text{Name} \) by the identity, and \( \_\_\uparrow1 \) by \( \text{Maybe} \). The same connection can be done with the \( \text{Fin} \) approach described in section 5.1.3 if one replaces \( \text{World} \) by \( \text{N} \), \( \text{Name} \) by \( \text{Fin} \), and \( \_\_\uparrow1 \) by \( \text{suc} \).
Our internal representation for worlds (section 4.1) using lists of boolean values is chosen to make \( \_+1 \) easy to define and to work with:

\[
\_+1 : \text{World} \rightarrow \text{World} \\
\alpha \_+1 = \text{false} :: \alpha
\]

We defined \( \_\uparrow1 \) on top of the primitive operators \( \_+1 \) and \( \_\triangleleft \). Unfolding \( \_\uparrow1 \) and \( \_\triangleleft \) shows the true nature of \( \_\uparrow1 \):

\[
\_\uparrow1\text{-is-true} : : \forall \{\alpha\} \rightarrow \alpha \_\uparrow1 \equiv \text{true} :: \alpha \\
\_\uparrow1\text{-is-true} : = \text{refl} \\
\quad -- \text{Since } \alpha \_\uparrow1 \text{ equals zero } \triangleleft \text{ false } :: \alpha \\
\quad -- \text{which reduces to true } :: \alpha
\]

These one-step definitions \( \_+1 \) and \( \_\uparrow1 \) are extended to any number to produce \( \_+W \) and \( \_\uparrow \) of type \( \text{World} \rightarrow \text{N} \rightarrow \text{World} \). The world \( \alpha \_+W^k \) is \( \alpha \_+1 \ldots \_+1 (\_+1 \text{ iterated } k \text{ times}) \) and the world \( \alpha \_\uparrow k \) is \( \alpha \_\uparrow1 \ldots \_\uparrow1 (_\uparrow1 \text{ iterated } k \text{ times}) \).

To the best of our knowledge, making the distinction between two forms of shifting operations for worlds (namely \( \_+1 \) and \( \_\uparrow1 \)) has never been investigated in the context of representing names and binders. As we see later in detail in section 5.4.3, this distinction is important and omitting it leads to less accurate types. Less accurate types led us to a broken definition of shifting in our first work on the subject [Pouillard and Pottier, 2010] as we detail in section 5.4.3.

\( \ell \)-bound and \( \ell \)-free names: In a context where we are working under \( \ell \) binders, we call \( \ell \)-bound, a name bound somewhere in the scope of \( \ell \) binders. We call \( \ell \)-free, a name that is free for all \( \ell \) binders. In other words, a de Bruijn index is \( \ell \)-bound if it is strictly less than \( \ell \); it is \( \ell \)-free otherwise.

\textbf{zero} \( ^N \): Since binders are not needed in the de Bruijn presentation, names are constructed directly. To start with, the simplest name is \textbf{zero} \( ^N \). The name \textbf{zero} \( ^N \) represents zero and inhabits any world shifted by one. While this is a primitive operation from a de Bruijn point of view, it can be defined in terms of our nominal interface:

\[
\text{zero} ^N : \forall \{\alpha\} \rightarrow \text{Name} \ (\alpha \_\uparrow1) \\
\text{zero} ^N = \text{name} ^B (0 ^B)
\]

The signatures of the core primitive operations on names are given in figure 5.1. One can add any constant to a name in any world with \textbf{add} \( ^N \). As-
5.2. AN INTERFACE FOR DE BRUIJN INDICES

\[
\text{add}^N : \forall \{\alpha\} \ k \to \text{Name} \ \alpha \\
\to \text{Name} \ (\alpha +^N k)
\]

\[
\text{subtract}^N : \forall \{\alpha\} \ k \to \text{Name} \ (\alpha +^N k) \\
\to \text{Name} \alpha
\]

\[
\text{cmp}^N : \forall \{\alpha\} \ \ell \to \text{Name} \ (\alpha \uparrow \ell) \\
\to \text{Name} \ ((\emptyset \uparrow \ell) \uplus \text{Name} \ (\alpha +^N \ell))
\]

\begin{align*}
\text{syntax add}^N & \quad \text{k x = x} +^N k \\
\text{syntax subtract}^N & \quad \text{k x = x} -^N k \\
\text{syntax cmp}^N & \quad \ell x = x <^N \ell
\end{align*}

Figure 5.1: Core operations on names

\[
\text{Name} \ (\emptyset +^N k) \\
\text{coerce}^N \\
\text{Name} \emptyset \quad \text{Name} \emptyset \perp \\
\text{coerce}^N \emptyset \subseteq \alpha \\
\text{Name} \alpha \\
\text{add}^N k \\
\text{subtract}^N k \\
\text{Name} \ (\alpha +^N k) \\
\text{coerce}^N \\
\text{Name} \ (\alpha \uparrow k) \\
\text{cmp}^N (if \geq k) \\
\text{Name} \ (\emptyset \uparrow k) \\
\text{coerce}^N \\
\text{Name} \ (\emptyset \uparrow k) \\
\text{Fin} \ k
\]

Figure 5.2: Operations on names
summing worlds are erased at run-time, by parametricity the resulting world of \( \text{add}^N \) clearly shows that this function does exactly its addition job. One can do the opposite operation with \( \text{subtract}^N \). Thanks to its precise type this function is total and the inverse of \( \text{add}^N \).

Given any world \( \alpha \), a name in the world \( \alpha \uparrow \ell \) is either strictly lower than \( \ell \) (and so also lives in \( \emptyset \uparrow \ell \)), or greater or equal to \( \ell \) (thus also lives in \( \alpha \uparrow^W \ell \)). This is exactly what the function \( \text{cmp}^N \ell \) is about. Given a name \( x \), \( \text{cmp}^N \ell x \) returns a disjoint sum of names which can be read in two parts. It first gives which side of the disjoint sum it stands, and second it gives a refined version of the input name \( x \).

Figure 5.2 depicts the different types of names we have and how our operations relates them. Starting from the bottom, names with worlds of the form \( \emptyset \uparrow k \) are definitely \( k \)-bound. Their value is completely known. The two arrows state the type isomorphism between \( \text{Name}(\emptyset \uparrow k) \) and \( \text{Fin} k \). Above we have names that may be bound or free (\( \text{Name}(\alpha \uparrow k) \)). A dynamic test (\( \text{cmp}^N \ell \)) can tell whether such a name is \( k \)-bound or not. Above we have names that are known to be greater than \( k \) (\( \text{Name}(\alpha \uparrow^W k) \)). They are \( k \)-free names. Above we have free names (\( \text{Name} \alpha \)). On the top we have impossible names since they are said to belong to an empty world. From them we can derive everything.

These primitive operations are enough to show an isomorphism between \( \text{Fin} n \) and \( \text{Name}(\emptyset \uparrow n) \). From this, every program involving \( \text{Fin} \) can be translated into our system. This means that our system does not restrict the programmer more than the \( \text{Fin} \) approach. However as soon as one uses finer types than \( \text{Name}(\emptyset \uparrow n) \), then fewer “wrong programs” type-check and more properties hold as we see in section 5.4.3.

We extend the inclusion relation with a set of new rules given in figure 5.3. The \( \subseteq \emptyset +1 \) rule states that \( \emptyset +1 \) is empty. Inclusion is preserved both ways by the contexts \( \uparrow 1 \) and \( \uparrow 1 +1 \). Finally \( \uparrow 1 +1 \) can be weakened to \( \uparrow 1 \). This accounts for the fact that \( \alpha \uparrow 1 \) means \( \{0\} \cup (\alpha +1) \) and so is a proper superset of \( \alpha +1 \). This set of rules is implemented according to the definition of inclusion, namely \( \forall x \rightarrow x \in \alpha \rightarrow x \in \beta \). On top of these base
rules, we derive others that we omit here (some are used in the code).

\[ \subseteq \downarrow \uparrow 1 \rightarrow \downarrow \uparrow 1 \text{ is derivable} \]
\[ \subseteq \downarrow \uparrow 1 \rightarrow \downarrow \uparrow 1 : \forall (\alpha \beta) \rightarrow \alpha \subseteq \beta \rightarrow \alpha \uparrow 1 \subseteq \beta \uparrow 1 \]
\[ \subseteq \downarrow \uparrow 1 \rightarrow \uparrow 1 = \subseteq \triangleleft 0 \]

5.2.1 Singleton worlds!

We said that our worlds denote finite subsets of \( \mathbb{N} \) and are more precise than in the Fin approach. Actually they can be as precise as we wish, since any subset of \( \mathbb{N} \) can be described by our operations on worlds (\( \emptyset, \_+1, \) and \( \_\uparrow 1 \)). In particular they can be singleton worlds. From singleton worlds we build singleton types for names:

\[
\text{World}^\sharp : \mathbb{N} \rightarrow \text{World} \\
\text{World}^\sharp n = \emptyset \uparrow 1 +^\sharp n \\
\text{Name}^\sharp : \mathbb{N} \rightarrow \text{Set} \\
\text{Name}^\sharp = \text{Name} \circ \text{World}^\sharp \\
\_\text{\_}^\mathbb{N} : \forall n \rightarrow \text{Name}^\sharp n \\
\_\text{\_}^\mathbb{N} n = \text{zero}^\mathbb{N} +^\mathbb{N} n
\]

Singleton worlds not only exist, they are also preserved by our two updating operations, namely \text{add}^\sharp and \text{subtract}^\sharp.

\[
\text{add}^\sharp : \forall \{n\} k \rightarrow \text{Name}^\sharp n \rightarrow \text{Name}^\sharp (k +^\mathbb{N} n) \\
\text{add}^\sharp \{n\} k x = \text{add}^\mathbb{N} k x \\
(-\text{because } \subseteq \text{-assoc+} \subseteq \text{-refl } n \ k \ -) \\
\text{subtract}^\sharp : \forall \{n\} k \rightarrow \text{Name}^\sharp (k +^\mathbb{N} n) \rightarrow \text{Name}^\sharp n \\
\text{subtract}^\sharp \{n\} k x = \text{subtract}^\mathbb{N} k x \\
(-\text{because } \subseteq \text{-assoc+}' \subseteq \text{-refl } n \ k \ -)
\]

5.3 Examples and advanced operations

5.3.1 Some convenience functions

Here are a few functions built on top of the interface (without using the concrete representation of names). \text{suc}^\mathbb{N} is \text{add}^\mathbb{N} 1 and \text{suc}^\_\text{\_}^\mathbb{N} \_\text{\_}^\uparrow 1 is a variant that includes a coercion from \( \alpha +1 \) to \( \alpha \uparrow 1 \). The function \_\text{\_}^\mathbb{N} turns a number \text{n}
into a name that inhabits any world with at least \( n + 1 \) consecutive binders.

\[
suc^N : \forall \{\alpha\} \to \text{Name} \alpha \to \text{Name} (\alpha +1) \\
suc^N = \text{add}^N 1
\]

\[
suc^\uparrow : \forall \{\alpha\} \to \text{Name} \alpha \to \text{Name} (\alpha \uparrow 1) \\
suc^\uparrow = \text{coerce}^N \subseteq+1\uparrow 1 \circ suc^N
\]

\[
\_^N : \forall \{\alpha\} n \to \text{Name} (\alpha \uparrow \text{suc} n) \\
\_^N \{\alpha\} n = \text{zero}^N \uparrow n
\]

(-because \( \alpha \uparrow 1 +^W n \subseteq \subseteq+\uparrow n \))

\[
\alpha \uparrow 1 \uparrow n \subseteq \subseteq-\text{exch}-\uparrow-\uparrow 1 n \\
\alpha \uparrow \text{suc} n \subseteq-)
\]

where open \( \subseteq-\text{Reasoning} \)

The function \( \text{subtract}^N \), similarly to the function \( \text{cmp} \), tells whether a given name is \( \ell \)-bound or \( \ell \)-free. In case the name is free, an “exported” version of it is returned. This function forms the base case of “exporting” functions such as \( \text{subtractTm}^D \) explained later on page 107. The function \( \text{pred}^N \) is a simple specialization of \( \text{subtract}^N \).

\[
\text{subtract}^N : \forall \{\alpha\} \ell \to \text{Name} (\alpha \uparrow \ell) \\
\to? \text{Name} \alpha
\]

\[
\text{subtract}^N \ell x \\
\text{with} \ x <^N \ell
\]

\[
\cdots \mid \text{inj}_1 - = \text{nothing} \\
\cdots \mid \text{inj}_2 x' = \text{just} (x' <^N \ell)
\]

\[
\text{pred}^N : \forall \{\alpha\} \to \text{Name} (\alpha \uparrow 1) \to? \text{Name} \alpha \\
\text{pred}^N \ell = \text{subtract}^N 1
\]

On top of \( \text{subtract}^N \), we also build a convenient eliminator for names which is simply the elimination of the result of \( \text{subtract}^N \).

\[
\text{subtractWith}^N : \forall \{\alpha \ A\} \ell \to A \to (\text{Name} \alpha \to A) \\
\to \text{Name} (\alpha \uparrow \ell) \to A
\]

\[
\text{subtractWith}^N \ell f = \text{maybe} f \circ \text{subtract}^N
\]

The function \( \text{shiftName} \ell k pf \) shifts its argument by \( k \) if this name is \( \ell \)-free, otherwise it leaves the \( \ell \)-bound name untouched. This function makes use of \( \text{cmp}^N \) and coerces the outputs to the required type. It also perform a
5.3. EXAMPLES AND ADVANCED OPERATIONS

coercion on the fly, giving extra flexibility for free.

\[ \text{shiftName} : \forall \{ \alpha \beta \} \ell k \to (\alpha \uparrow^k k) \subseteq \beta \]
\[ \rightarrow \text{Name} (\alpha \uparrow \ell) \]
\[ \rightarrow \text{Name} (\beta \uparrow \ell) \]

\[ \text{shiftName} \ell k pf x \]
\[ \text{with } x <^N \ell \]
\[ \ldots \mid \text{inj} 1 \ x' = x' \quad \langle \text{because pf}_1 \rangle \quad \ell\text{-bound} \]
\[ \ldots \mid \text{inj} 2 \ x' = x' \uparrow^k k \quad \langle \text{because pf}_2 \rangle \quad \ell\text{-free} \]

\text{where}
\[ \text{pf}_1 = \subseteq\text{-cong} \uparrow \subseteq - 0 \ell \]
\[ \text{pf}_2 = \subseteq\text{-trans} (\subseteq\text{-exch} \uparrow \subseteq \text{refl} \ell k) \]
\[ (\subseteq\text{-ctx} \uparrow pf \ell) \]

The function \text{protect}↑ shifts a name transformer. Let \( f \) be a function from names to names. The function \text{protect}↑ \ell f is a version of \( f \) that is applicable under \( \ell \) binders. That is, if \( f \) has type \( \text{Name} \alpha \to \text{Name} \beta \) then \text{protect}↑ \ell f has type \( \text{Name} (\alpha \uparrow \ell) \to \text{Name} (\beta \uparrow \ell) \). Let \( x \) be a name under \( \ell \) binders. When \( x \) is \( \ell \)-bound, it is left untouched by \text{protect}↑. When \( x \) is \( \ell \)-free, we can subtract \( \ell \) to \( x \), give it to \( f \), and then add \( \ell \) to get the result.

\[ \text{protect}↑ : \forall \{ \alpha \beta \} \ell \]
\[ \rightarrow (\text{Name} \alpha \to \text{Name} \beta) \]
\[ \rightarrow (\text{Name} (\alpha \uparrow \ell) \to \text{Name} (\beta \uparrow \ell)) \]

\[ \text{protect}↑ \ell f x \]
\[ \text{with } x <^N \ell \]
\[ \ldots \mid \text{inj} 1 \ x' = x' \quad \langle \text{because } \subseteq\text{-cong} \uparrow \subseteq - 0 \ell \rangle \]
\[ \ldots \mid \text{inj} 2 \ x' = f (x' \uparrow^k k) \uparrow^N \ell \]
\[ \langle \text{because } \subseteq\text{-++} \uparrow \ell \rangle \]

By combining \text{protect}↑ and \text{add}^k one obtains an alternative implementation of \text{shiftName} called \text{shiftName}'. However \text{shiftName}' is more efficient since it avoids to subtracting \( \ell \) to add it back after adding \( k \).

\[ \text{shiftName}' : \forall \{ \alpha \beta \} \ell k \to (\alpha \uparrow^k k) \subseteq \beta \]
\[ \rightarrow \text{Name} (\alpha \uparrow \ell) \to \text{Name} (\beta \uparrow \ell) \]

\[ \text{shiftName}' \ell k pf = \text{protect}↑ (\text{coerce}^k pf \circ \text{add}^k k) \ell \]
5.3.2 Building terms

Building terms with our de Bruijn style library is as easy as building them in a plain de Bruijn index representation. The structure is exactly the same, and the variables are made of numbers (of type \( N \)) using \( N \). Below we define representations of the identity function as \( \text{idTm}^D \), the application operator as \( \text{appTm}^D \), and the composition function as \( \text{compTm}^D \):

\[
\text{idTm}^D : \forall \{ \alpha \} \rightarrow \text{Tm}^D \alpha \\
\text{idTm}^D = \chi(V(0^N))
\]

\[
\text{appTm}^D : \forall \{ \alpha \} \rightarrow \text{Tm}^D \alpha \\
\text{appTm}^D = \chi(\chi(V(1^N) \cdot V(0^N)))
\]

\[
\text{compTm}^D : \forall \{ \alpha \} \rightarrow \text{Tm}^D \alpha \\
\text{compTm}^D = \chi(\chi(\chi(V(2^N)) \cdot (V(1^N) \cdot V(0^N))))
\]

5.3.3 Computing free variables

Our first example of functions over terms computes a list of the free variables in the input term. The function \( \text{fv}^D \) below, while straightforward, has the subtle cases of binding constructs (\( \chi \) here). In these cases we have to remove the bound name from the list of free variables produced by the recursive call. In this nameless representation this amounts to removing occurrences of 0 and subtracting 1 to other name occurrences. This is done by the function \( \text{rm}_0 \) which calls \( \text{pred}^N \) on each element of the list and merges the results. Note that forgetting to remove the bound variable results in a type error. In the same vein the typing of \( \text{fv}^D \) ensures that all returned variables do appear free in the given term.

\[
\text{rm}_0 : \forall \{ \alpha \} \rightarrow \text{List} \, (\text{Name} (\alpha \uparrow 1)) \\
\text{rm}_0 = [] \\
\text{rm}_0 \, (x :: xs) \text{ with } \text{pred}^N \, x \\
... \quad | \quad \text{just } x' = x' :: \text{rm}_0 \, xs \\
... \quad | \quad \text{nothing } = \text{rm}_0 \, xs
\]
5.3. EXAMPLES AND ADVANCED OPERATIONS

fv\^D : ∀ \{α\} → Tm\^D α → List (Name α)
fv\^D (V x) = [x]
fv\^D (fct · arg) = fv\^D fct ++ fv\^D arg
fv\^D (λ t) = rm_0 (fv\^D t)
fv\^D (Let t u) = fv\^D t ++ rm_0 (fv\^D u)

5.3.4 Generic traversal

As with the nominal approach (3.2) we build a generic traversal function to avoid code duplication among various operations on terms. However in this nameless style the matter is simplified. The information to carry down during the traversal can be summarized by a single natural number, namely the \(\ell\) parameter that we have already used. This parameter records how many binders have been entered.

```haskell
module TraverseTm\^D
(E) (E-app : Applicative E)
{α β} (trName : ∀ \ell → Name (α ↑ \ell) → E (Tm\^D (β ↑ \ell)))
where
open Applicative E-app

tr : ∀ \ell → Tm\^D (α ↑ \ell) → E (Tm\^D (β ↑ \ell))
tr \ell (V x) = trName \ell x
tr \ell (t · u) = pure _·_ ⊕ tr \ell t ⊕ tr \ell u
tr \ell (λ t) = pure λ ⊕ tr (suc \ell) t
tr \ell (Let t u) = pure Let ⊕ tr \ell t ⊕ tr (suc \ell) u

trTm\^D : Tm\^D α → E (Tm\^D β)
trTm\^D = tr 0
```

Like in section 3.2 we made a special case for variable occurrences: \(\text{trName}\) is not wrapped with the constructor \(V\). Mapping names to terms yields capture-avoiding substitution almost for free. However, in the meantime we build \(\text{trTm}^D\) which maps names to names. It does so by applying \text{pure} \(V\) to the name-to-name function:
open TraverseTm^b

trTm^D : 
∀ {E} (E-app : Applicative E) {α β} 
(trName : ∀ ℓ → Name (α ↑ ℓ) 
→ E (Name (β ↑ ℓ))) 
→ Tm^D α → E (Tm^D β) 
trTm^D E-app trName = trTm^D E-app (λ ℓ x → pure V ⊗ trName ℓ x) 
where open Applicative E-app

Renaming functions: In many functions over terms the handling of variables shares a common part. Given a variable under ℓ binders, we test if the variable is ℓ-bound. If so we leave it untouched, otherwise we subtract ℓ and go on a specific processing after which we add ℓ again to the free variables of the result. The traversal function is augmented by this processing of bound variables to build renameTm^DA:

-- Like protect↑ but generalized to Applicative functors
protect↑A = {! omitted !}

renameTm^DA : ∀ {E} (E-app : Applicative E) 
{α β} (θ : Name α → E (Name β)) 
→ Tm^D α → E (Tm^D β) 
renameTm^DA E-app θ = trTm^D E-app (protect↑A E-app θ)

Then by picking either the identity functor (id-app), or the Maybe one we build two functions (a total and a partial one) to perform any renaming, namely renameTm^D and renameTm^D?:

renameTm^D : ∀ {α β} → (Name α → Name β) 
→ Tm^D α → Tm^D β 
renameTm^D = trTm^D id-app ◦ protect↑ 
-- or
-- renameTm^D = renameTm^DA id-app

renameTm^D? : ∀ {α β} → (Name α →? Name β) 
→ Tm^D α →? Tm^D β 
renameTm^D? = renameTm^DA Maybe.applicative
Lifting name functions: Any operation on names can now be lifted to terms. The function \( \text{addTm}^D \) lifts the function \( \text{add}^N \) from names to terms. It takes a number \( k \) and a term and adds \( k \) to all the free variables:

\[
\text{addTm}^D : \forall \{ \alpha \} \ k \to \text{Tm}^D \alpha \to \text{Tm}^D (\alpha +^k) \\
\text{addTm}^D = \text{renameTm}^D \circ \text{add}^N
\]

The functions \( \text{subtractTm}^D \) and \( \text{subtractTm}^D? \) respectively lift the functions \( \text{subtract}^N \) and \( \text{subtract}^N? \) from names to terms. They enable to subtract a number \( k \) to all the free variables of a term:

\[
\text{subtractTm}^D : \forall \{ \alpha \} \ k \to \text{Tm}^D (\alpha +^W k) \to \text{Tm}^D \alpha \\
\text{subtractTm}^D = \text{renameTm}^D \circ \text{subtract}^N
\]

\[
\text{subtractTm}^D? : \forall \{ \alpha \} \ \ell \to \text{Tm}^D (\alpha \uparrow \ell) \to ? \text{Tm}^D \alpha \\
\text{subtractTm}^D? = \text{renameTm}^D? \circ \text{subtract}^N?
\]

While \( \text{coerce}^N \) can be lifted to terms in the same way, we can by-pass the \( \text{protect}^\uparrow \) dynamic tests and directly “protect” the inclusion witness with an appropriate inclusion rule. Put differently there are two ways to go from a proof \( \text{pf} \) of \( \alpha \subseteq \beta \) to \( \text{Name} (\alpha \uparrow \ell) \to \text{Name} (\beta \uparrow \ell)) \): one is to protect the result of \( \text{coerce} (\text{protect}^\uparrow \circ \text{coerce}^N \text{pf}) \) and the other is to coerce with protected inclusion witness \( (\text{coerce}^N \circ \subseteq\text{-cong}^\uparrow \text{pf}) \):

\[
\text{coerceTm}^D : \forall \{ \alpha \beta \} \rightarrow \alpha \subseteq \beta \rightarrow \text{Tm}^D \alpha \rightarrow \text{Tm}^D \beta \\
\text{coerceTm}^D \text{pf} = \text{trTm}^D \text{id-app} (\text{coerce}^N \circ \subseteq\text{-cong}^\uparrow \text{pf}) \\
-- \text{or less efficiently:} \\
-- \text{coerceTm}^D = \text{renameTm}^D \circ \text{coerce}^N
\]

Lifting \( \text{add}^N \) to terms can be done more efficiently as well. Indeed \( \text{addTm}^D \) internally uses \( \text{renameTm}^D \) which uses \( \text{protect}^\uparrow \). Here the dynamic test performed by \( \text{protect}^\uparrow \) is necessary. However when the name is \( \ell \)-free we subtract \( \ell \) and add it back after adding \( k \). The function \( \text{shiftName} \) avoids this extra computation, hence the following \( \text{shiftTm}^D \):

\[
\text{shiftTm}^D : \forall \{ \alpha \beta \} \ k \rightarrow (\alpha +^W k) \subseteq \beta \rightarrow \text{Tm}^D \alpha \rightarrow \text{Tm}^D \beta \\
\text{shiftTm}^D \text{ pf} = \text{trTm}^D \text{id-app} (\lambda \ell \rightarrow \text{shiftName} \ell \ k \text{ pf}) \\
-- \text{or less efficiently:} \\
-- \text{shiftTm}^D \text{ pf} = \text{renameTm}^D \circ \text{coerce}^N \text{ pf} \circ \text{add}^N \text{ k}
\]

The function \( \text{closeTm}^D? \) is built like in nominal style (section 3.2):

\[
\text{closeTm}^D? : \forall \{ \alpha \} \rightarrow \text{Tm}^D \alpha \rightarrow ? \text{Tm}^D \emptyset \\
\text{closeTm}^D? = \text{renameTm}^D? \ (\text{const nothing}) -- \text{any free var leads to a failure}
Capture avoiding substitution. To implement capture avoiding substitution for the type \( \text{Tm}^D \), all we need is a specific function \( \text{trName} \) for \( \text{trTm}^D \). Here substitutions are represented as functions from names to terms. The function \( \text{substVarTm}^D \) handles the case for variables. This function is very close to \( \text{protect} \uparrow \) but extended to functions returning terms.

\[
\text{substVarTm}^D : \forall \{ \alpha \ \beta \} \to (\text{Name} \ \alpha \to \text{Tm}^D \ \beta) \to \forall \ \ell \to \text{Name} (\alpha \uparrow \ell) \to \text{Tm}^D (\beta \uparrow \ell)
\]

\[
\text{substVarTm}^D f \ \ell \ x \quad \text{with} \quad x <^N \ell
\]

\[
\ldots \mid \text{inj}_1 x' = V (x' \quad \text{(-because } \subseteq \text{-cong-} \uparrow \subseteq \Theta \ \ell \ -))
\]

\[
\ldots \mid \text{inj}_2 x' = \text{shiftTm}^D \ell (\subseteq^{-+} \uparrow \ell) (f (x' \triangleleft \ell))
\]

The main function \( \text{substTm}^D \) instantiates \( \text{trTm}^D \) with the identity applicative functor and \( \text{substVarTm}^D \):

\[
\text{substTm}^D : \forall \{ \alpha \ \beta \} \to (\text{Name} \ \alpha \to \text{Tm}^D \ \beta) \to (\text{Tm}^D \ \alpha \to \text{Tm}^D \ \beta)
\]

\[
\text{substTm}^D = \text{trTm}^D \text{id-app} \circ \text{substVarTm}^D
\]

As an illustration, the function \( \beta\text{-red}^D \) performs a \( \beta \)-reduction at the root of the term using the function \( \text{substTm}^D \):

\[
\beta\text{-red}^D : \forall \{ \alpha \} \to \text{Tm}^D \ \alpha \to \text{Tm}^D \ \alpha
\]

\[
\beta\text{-red}^D (\lambda \ fct \cdot \ arg) = \text{substTm}^D (\text{subtractWith}^N 1 \ arg \ V) \ fct
\]

\[
\beta\text{-red}^D \ t = t
\]

5.3.5 Nameless term comparison

We show that all the subtle work is done at the level of names in a separate and reusable function called \( \text{cmpName} \uparrow \). This function takes a function that compares two free names and builds one that compares two names under \( \ell \) bindings. It does so by comparing both of them to \( \ell \). If they are both bound they can be safely compared using \( ==^N \) since they now are of the same type. If they are both free, they can be compared using the function received as argument. Otherwise they are different.

\[
\text{cmpName} \uparrow : \forall \{ \alpha \ \beta \} \ \ell \to \text{Cmp} \ | \text{Name} \ \alpha \ \beta
\]

\[
\text{cmpName} \uparrow \ell \ \Gamma \ x \ y \ \text{with} \ x <^N \ell \ | \ y <^N \ell
\]

\[
\ldots \mid \text{inj}_1 x' \ | \ \text{inj}_1 y' = x' ==^N y'
\]

\[
\ldots \mid \text{inj}_2 x' \ | \ \text{inj}_2 y' = \Gamma (x' \triangleleft \ell) (y' \triangleleft \ell)
\]

\[
\ldots \mid \_ \ | \ _ = \text{false}
\]
The function \( \text{cmpTm} \) structurally compares two terms in a simple way, only keeping track of the number of traversed binders and calling \( \text{cmpName} \) at variables:

\[
\text{cmpTm} : \forall \{\alpha \beta\} \rightarrow |\text{Cmp}| \text{Name} \alpha \beta \rightarrow |\text{Cmp}| \text{Tm} \alpha \beta
\]

\[
\text{cmpTm}(\alpha) \{\beta\} \Gamma = \text{go } 0 \text{ where } \\
go : \forall \ell \rightarrow |\text{Cmp}| \text{Tm} \alpha \beta \rightarrow |\text{Cmp}| \text{Tm} \alpha \beta \\
go \ell (V x) (V y) = \text{cmpName} \ell \Gamma x y \\
go \ell (t \cdot u) (v \cdot w) = \text{go} \ell t v \land \text{go} \ell u w \\
go \ell (\lambda t) (\lambda u) = \text{go} (\text{suc} \ell) t u \\
go \ell (\text{Let } t u) (\text{Let } v w) = \text{go} \ell t v \land \text{go} (\text{suc} \ell) u w \\
go \_ \_ \_ \_ = \text{false}
\]

By instantiating the name comparator \( \Gamma \) by the homogeneous name comparison function \( \_ == \_ \_ \) we get an equality test on nameless terms. While this function works on open terms, they are requested to inhabit a common world.

\[
\_ == \_ \_ \_ : \forall \{\alpha\} \rightarrow |\text{Cmp}| \text{Tm} \alpha \alpha \\
\_ == \_ \_ \_ = \text{cmpTm} \_ == \_ \_ \_ 
\]

However in the particular case of comparing terms in a common world, we can define a simpler and a little faster equality test on terms. To do so we exploit the fact that the name abstraction is canonical and thus the term comparison is kept homogeneous during the whole comparison. In particular the function \( \text{cmpName} \) is not used.

\[
\_ == \_ : \forall \{\alpha\} \rightarrow |\text{Cmp}| \text{Tm} \alpha \alpha \\
\_ == \_ (V x) (V y) = x == y \\
\_ == \_ (t \cdot u) (v \cdot w) = \_ == \_ t v \land \_ == \_ u w \\
\_ == \_ (\lambda t) (\lambda u) = \_ == \_ t u \\
\_ == \_ (\text{Let } t u) (\text{Let } v w) = \_ == \_ t v \land \_ == \_ u w \\
\_ == \_ = \text{false}
\]

5.4 Logical Relations for de Bruijn indices

5.4.1 Relations for the de Bruijn world operations

We now have to define how our operation on worlds fits the logical relation. Figure 5.4 depicts how the operators \( \_ [+] 1 \) and \( \_ [\uparrow] 1 \) apply to the graph of a relation.
5.4.2 De Bruijn functions fit the relation

We now give a short overview of the proofs needed to show that our functions fit the relation. Thanks to the definition of \( \alpha_r \) \([+1]\) and \([\uparrow 1]\), \(\text{add}^N k\) and \(\text{subtract}^N k\) fit the relation. These two are later extended to \(\text{add}^N k\) and \(\text{subtract}^N k\) by an induction on \(k\). Here are for instance the type signatures for \(\text{add}^N\) and \(\text{cmp}^N\):

\[
\text{add}^N : (\forall (\alpha_r : \text{World}) \Rightarrow \Rightarrow) \\
\quad \langle k_r : \text{N} \rangle \Rightarrow \Rightarrow) \\
\quad \langle \text{Name} (\alpha_r \uparrow) \rangle \Rightarrow \\
\quad \langle \text{Name} (\alpha_r [+]) k_r \rangle \rangle \\
\]

\[
\text{cmp}^N : (\forall (\alpha_r : \text{World}) \Rightarrow \Rightarrow) \\
\quad \langle k_r : \text{N} \rangle \Rightarrow \Rightarrow) \\
\quad \langle \text{Name} (\alpha_r \uparrow) k_r \rangle \Rightarrow \\
\quad \langle \text{Name} (\emptyset \uparrow) k_r \rangle \rangle \\
\quad \langle \text{Name} (\alpha_r [+]) k_r \rangle \rangle \\
\]

The definition of \(\text{cmp}^N\) is not a simple induction on its first argument. It calls \(\preceq\) (which does an induction) and returns a Boolean value. Based on this Boolean value, the function \(\text{cmp}^N\) returns either \(\text{inj}_1\) or \(\text{inj}_2\) (the constructors of \(\uplus\)) with the same name (with a different proof). To prove \([\text{cmp}^N]\) we show the equivalence with a simpler inductive function and show that this simpler function is in the relation. Thanks to the ex-
5.4. LOGICAL RELATIONS FOR DE BRUIJN INDICES

We have shown that the new inclusion rules (Figure 5.3) fit the relation.

5.4.3 On the strength of free theorems

Every well-typed term comes with a free theorem (section 4.2.1). However depending on the type of the term the strength of the theorem varies a lot. For instance at type \( \mathbb{N} \) the theorem only tell that the term is equal to itself. At type \( \mathbb{N} \to \text{Bool} \) the theorem says no more than the function is deterministic. At type \( \forall \{ A : \text{Set} \} \to A \to A \) it says that the function behaves as the identity function, which is much stronger. We now give a few elements of what can affect the strength of free theorems in our context. We continue to use our type \( \text{Tm}^D \) to represent some data structures with names and binders but it could be any other. Moreover we focus on functions from terms to terms, where the input and the output worlds are the same. We discuss the strength of the abstraction level of the input or output term of such a function. From this perspective figure 5.5 depicts the relation corresponding to these types.

Various term types  The weakest type we can give to a function taking a term with names and binders is \( \forall \{ \ell \} \to \text{Tm}^D (\emptyset \uparrow \ell) \to \ldots \). A term re-

Figure 5.5: Various term types: from concrete to abstract

tensionality of the logical relation, no additional axiom is required to show that \( \text{cmp}^D \) fits the relation.

We have shown that the new inclusion rules (Figure 5.3) fit the relation.
ceived by such a function can have a statically unknown number of distinct free variables, but we know that these variables are comprised in the interval \([0 .. ℓ-1]\). The free theorem of \(∀{ℓ} \rightarrow \text{Tm}^D (\emptyset ↑ ℓ) \rightarrow \text{Tm}^D (\emptyset ↑ ℓ)\) says no more than “the function is deterministic” because the logical relation \([\text{Tm}^D] (\emptyset ↑ ℓ)\) is the identity. We also know because of typing that the resulting term cannot have ℓ-free occurrences.

The type \(\text{Tm} (α ↑ ℓ)\) is more abstract than \(\text{Tm}^D (\emptyset ↑ ℓ)\), an unknown world is used instead of the empty world. However this type still shows a known amount of bindings. Then, a function of type \(∀{α ℓ} \rightarrow \text{Tm}^D (α ↑ ℓ) \rightarrow \text{Tm}^D (α ↑ ℓ)\) has a stronger free theorem than the previous one. It says that the function commutes with a renaming of the variables in the world α (section 5.4.4). This is a common type to deal with open terms under a partial environment:

\[
\text{some-op} : ∀{α ℓ} \rightarrow (\text{Fin} ℓ \rightarrow \text{Info}) \rightarrow \text{Tm}^D (α ↑ ℓ) \rightarrow \text{Tm}^D (α ↑ ℓ)
\]

\[
\text{some-op} Γ t = \{! omitted !\}
\]

The most abstract type for terms makes no assumptions on their free variables. This can be done by quantifying by an arbitrary world. The free theorem associated with the type \(∀ {α} \rightarrow \text{Tm}^D α → \text{Tm}^D α\) is then stronger and says that the function commutes with any renaming of the free variables. This particular type is studied in detail in section 5.4.4.

**Extra arguments** Note that adding extra arguments to a function can drastically affect the strength of its free theorem. An extreme example is the type \(∀{α} \rightarrow (α ≡ \emptyset) \rightarrow \text{Tm}^D α → \text{Tm}^D α\), which is ruined by its α ≡ ∅ argument. This argument makes the type equivalent to \(\text{Tm}^D \emptyset → \text{Tm}^D \emptyset\) which has a trivial free-theorem. While the above example is extreme, this is an important point to watch out for when adding extra arguments to a function. Another example is the type \(∀{α β} → \text{Tm}^D α → \text{Tm}^D β → \text{Tm}^D β\) versus \(∀{α β} → (\text{Name} α → \text{Name} β → \text{Bool}) → \text{Tm}^D α → \text{Tm}^D β → \text{Tm}^D β\). The first one cannot compare the free variables of the two given terms while the second can apply a user-supplied function to do so.

**Shifting versus adding** Last but not least using \(α^W\) instead of \(α↑\) significantly improves the strength of the associated free theorem. Consider the function \(\text{protectedAdd}\):

\[
\text{protectedAdd} : ∀ {α} ℓ k → \text{Name} (α ↑ ℓ)
\]

\[
→ \text{Name} (α ^W k ↑ ℓ)
\]

\[
\text{protectedAdd} ℓ k = \text{protect}↑ ℓ (\text{add}^W k)
\]

The following diagram depicts the graph behind the function \(\text{protectedAdd} ℓ k\):
Consider now a weaker type, namely:

\[
\text{protectedAdd}^{\uparrow} : \forall \{\alpha\} \ell \ k \rightarrow \text{Name} (\alpha \ ^{\uparrow} \ell) \\
\rightarrow \text{Name} (\alpha \ ^{\uparrow} k \ ^{\uparrow} \ell)
\]

\[
\text{protectedAdd}^{\uparrow} \ k = \text{protect}^{\uparrow} \ell (\text{add}^{\uparrow} \ k)
\]

We depict the graph behind the function \text{protectedAdd}^{\uparrow}. The graph is actually the same than the graph for the function \text{protectedAdd}. We extend the set of nodes to match the codomain stated by the type.

We simply replaced the occurrence of \(_{\ ^{\uparrow}W}\) by \(_{\ ^{\uparrow}L}\). The consequences of this change are disastrous: this type allows more behaviors for its functions. Indeed the \text{add}^{\uparrow} k function can be given the latter type (but not the former) when using the appropriate inclusion witness to exploit the commutativity of \(_{\ ^{\uparrow}L}\).
CHAPTER 5. THE DE BRUIJN APPROACH

unprotectedAdd : ∀ {α} k ℓ → Name (α ↑ ℓ) → Name (α ↑ k ↑ ℓ)

unprotectedAdd k ℓ
= coerce nit-exch↑↑ℓ k) ◦ add nit k

-- this is ok since (α ↑ k) ↑ ℓ ≡ (α ↑ ℓ) ↑ k

-- whereas (α + nit k) ↑ ℓ ≢ (α ↑ ℓ) + nit k

In our previous work [Pouillard and Pottier, 2010] we had a function called shiftName which was incorrectly defined with the unprotectedAdd behavior. Indeed the correct expected behavior is the one of protectedAdd↑. In this paper we had only the ↑ operation, and thus we missed the finer type we can give to protectedAdd. It took us a long time to discover this mistake, since we thought that our logical relation argument was enough. The logical relations proofs were indeed correct, the free-theorem were also correct but were not always “saying” what we expected. In summary we want to highlight that all the logical relations results have to be taken with great care. A weaker function type than expected can ruin the intended informal properties.

5.4.4 Using logical relations and parametricity

To formally show that a world-polymorphic function f of type ∀ {α} → TmB α → TmB α commutes with a renaming of the free variables, we proceed as follows. First we recall the natural definition of logical relation on the type TmB. Second we present the type Ren of renamings as injective functions. Third renaming is shown equivalent to being related at the type TmB. Finally we prove our commutation lemma by using the free-theorem associated to the function f.

The logical relation for the type TmB is mechanical. It states that two terms are related if they have the same structure and related free variables:
5.4. LOGICAL RELATIONS FOR DE BRUIJN INDICES

\[\text{data } [[\text{Tm}^\alpha]] \{\alpha_1 \alpha_2\} (\alpha_r : [[\text{World}]] \alpha_1 \alpha_2) :
\]
\[\text{Tm}^\alpha \alpha_1 \to \text{Tm}^\alpha \alpha_2 \to \text{Set where}
\]
\[\text{[[V]]} : \forall \{x_1 x_2\} (x_r : [[\text{Name}]] \alpha_r x_1 x_2) 
\]
\[\to [[\text{Tm}^\alpha]] \alpha_r (V x_1) (V x_2)
\]
\[\text{[[.]_\text{Let}} : \forall \{t_1 t_2 u_1 u_2\}
\]
\[\{t_r : [[\text{Tm}^\alpha]] \alpha_r t_1 t_2
\]
\[u_r : [[\text{Tm}^\alpha]] \alpha_r u_1 u_2
\]
\[\to [[\text{Tm}^\alpha]] \alpha_r (t_1 \cdot u_1) (t_2 \cdot u_2)
\]
\[\text{[[x]]} : \forall \{t_1 t_2\} (t_r : [[\text{Tm}^\alpha]] (\alpha_r [↑1]) t_1 t_2)
\]
\[\to [[\text{Tm}^\alpha]] \alpha_r (x t_1) (x t_2)
\]

In the following, we choose a “renaming” to be an injective function \(\Phi\) of names to names. The type of a renaming that maps names in the world \(\alpha\) to names in the world \(\beta\) is \(\text{Ren} \alpha \beta\). Note that there is a slight difference between a renaming from \(\alpha\) to \(\beta\) (\(\text{Ren} \alpha \beta\)) and the worlds \(\alpha\) and \(\beta\) being “related” (\([[[\text{World}]]\alpha \beta\)). On renamings, we define three functions \(\langle\_\rangle^\text{N}, \langle\_\rangle^\text{W}\) and \(\langle\_\rangle^\text{Tm}\) which respectively turn a renaming into a function of names to names, into a relation between worlds, and into a function of terms to terms.

\[\text{Ren} : (\alpha_1 \alpha_2 : \text{World}) \to \text{Set}
\]
\[\text{Ren} \alpha_1 \alpha_2 = \text{Injection} (\text{Nm} \alpha_1) (\text{Nm} \alpha_2)
\]
\[\text{-- } \ast \text{ Injection From To is the set of the injective functions}
\]
\[\text{-- from the setoid From to the setoid To.}
\]
\[\text{-- } \ast \text{ Nm } \alpha \text{ is the setoid on Name } \alpha
\]

\[\langle\_\rangle^\text{W} : \forall \{\alpha \beta\} \to \text{Ren } \alpha \beta \to (\alpha \to^\text{W} \beta)
\]
\[\langle \Phi \rangle^\text{W} = \{! \text{ omitted }!\} \text{ -- Projects out the function over names}
\]

\[\langle\_\rangle^\text{W} (\alpha) \{\beta\} \Phi = \mathcal{R}, \mathcal{R}\text{-pres-}\equiv
\]
\[\text{where } \mathcal{R} : \text{Name } \alpha \to \text{Name } \beta \to \text{Set}
\]
\[\mathcal{R} x y = (\Phi)^\text{W} x \equiv y
\]
\[\mathcal{R}\text{-pres-}\equiv : \text{ Preserve-}\equiv \mathcal{R}
\]
\[\mathcal{R}\text{-pres-}\equiv = \{! \text{ omitted }!\}
\]

\[\langle\_\rangle^\text{Tm} : \forall \{\alpha \beta\} \to \text{Ren } \alpha \beta \to (\text{Tm}^\alpha \alpha \to \text{Tm}^\beta \beta)
\]
\[\langle \Phi \rangle^\text{Tm} = \text{renameTm}^\alpha (\Phi)^\text{W}
\]

We now observe that given a renaming \(\Phi\), it is equivalent for two terms \(t_1\) and \(t_2\) to be related by \([[[\text{Tm}^\alpha]]\{\Phi\}^\text{W}\) and for \(t_2\) to be equal to \(t_1\) renamed.
with Φ. Put differently at the type \( Tm \) the relation coincides with the \( \alpha \)-equivalence (using the identity renaming for \( Φ \)).

\[
\text{Rename} : \forall\ \{α, β\} \rightarrow \text{Ren} \ α \ β \rightarrow Tm^D \ α \rightarrow Tm^D \ β \rightarrow \text{Set}
\]

\[
\text{Rename } Φ \ t_1 \ t_2 = (Φ)^Tm \ t_1 ≡ t_2
\]

\[
[Tm^D] \leftrightarrow \text{Rename} : \forall\ \{α, β\} \ (Φ : \text{Ren} \ α \ β) \rightarrow [Tm^D] \ (Φ) \leftrightarrow \text{Rename} \ Φ
\]
Finally given a function $f$ and a proof $f_r$ that $f$ is in the logical relation, we can show that any renaming $\Phi$ commutes with the function $f$. To prove this we apply our $\llbracket \text{Tm}^D \rrbracket \leftrightarrow \text{rename}$ lemma in both directions and use $f_r$ with the renaming $\Phi$ lifted as a $\llbracket \text{World} \rrbracket$.

\[ \text{-- Pointwise equality} \]
\[ f \equiv g = \forall x \rightarrow f \ x \equiv g \ x \]

\[
\text{ren-comm} : (f : \forall \{\alpha\} \rightarrow \text{Tm}^D \alpha \rightarrow \text{Tm}^D \alpha)
\]
\[
(f_r : (\forall (\alpha : \text{World}) \rightarrow \llbracket \text{Tm}^D \rrbracket \alpha_r [\rightarrow] \llbracket \text{Tm}^D \rrbracket \alpha_r) \ f \ f)
\]
\[
\{\alpha \beta : \text{World}\} (\Phi : \text{Ren} \alpha \beta)
\]
\[
\rightarrow (\llbracket \text{Tm} \rrbracket \circ f \equiv f \circ (\llbracket \text{Tm} \rrbracket \Phi) \rightarrow f) \]

\[
\text{ren-comm } f f_r \Phi \ t
\]
\[ = \llbracket \text{Tm}^D \rrbracket \rightarrow \text{Rename} \ \Phi \ (f_r \ (\Phi) \llbracket \text{Tm}^D \rrbracket \Phi \equiv \text{refl}) \]

Chapter 6

Variations and Related Work

This chapter covers various experimentations and connects our approach to more existing work. While some of the connections are not fully developed, they show the path to a complete connection and still give some insight.

The chapter is structured as follows. The first section explores the use of atoms as a separate kind of global names. In this section we explain the construction of Locally Nameless and Locally Named libraries where the type for global names is Atom and the type for local names is our type Name. We discuss the limitations of these approaches as programming interfaces, but underline the complementary role they can have when combined with our library.

In section 6.2 we describe another nameless approach from N.G. de Bruijn [de Bruijn, 1972] that is now called “de Bruijn levels”. We show how our existing library accommodates this style with only the addition of two inclusion rules.

In section 6.3 we describe a common interface for binders called links. This interface revives the presentation of our previous work [Pouillard and Pottier, 2010]. We show how the “unifying” part of this link-based approach can be integrated in our library. This approach enables greater code re-use without sacrificing much of the flexibility of our approach.

In section 6.4 we briefly explore how different approaches can be combined in order to be used at the same time. To illustrate this we combine nominal and de Bruijn indices in the same data type. This could allow for instance to convert a subterm to de Bruijn indices in order to apply a given algorithm.

In section 6.5 we cover a series of description languages used to describe “nominal types”. We show how the use of our explicit worlds can cope with pretty much everything these languages can describe. To do so we explain how each construct of these description languages can be expressed with worlds.

Section 6.6 discusses some more related work. We focus on relatively
recent work with which we have not yet drawn a concrete connection so far.

6.1 Dynamically stratified representations

Well known techniques such as *Locally Nameless* [Charguéraud, 2011, Aydemir et al., 2008], or *Locally Named* [Pollack et al., 2011, Sato and Pollack, 2010] can be qualified as “dynamically stratified representations”. Indeed these techniques use a double representation of variables, one for *local* variables, and one for *global* variables. The idea is to use local variables as the internal representation of the binding structure and to provide operations to switch back and forth from local to global variables. Name abstractions are introduced with the *close* operation. Given a subterm \( t \) and a global name \( X \), a name abstraction is built by picking a local name \( x \) and replacing \( X \) by \( x \) in \( t \), to form the body of the newly created name abstraction. Conversely, to *open* a name abstraction, one gives a global name \( X \) and an abstraction to be opened. The abstraction is internally made of a local name \( x \) and a subterm \( t \). The opening operation returns \( t \) where \( X \) replaces \( x \).

The main purpose of this double representation is to hide the handling of local names to the client and to let the client use only global names. To be sure to never encounter a local name, we want our terms to be *locally closed*, meaning without any free local variables. This property guarantees that starting from a locally closed term and properly opening abstractions, we never reach a local variable. Hence we only deal with global variables and avoid the hard work implied by local names and their abstractions.

While the representation for local names distinguishes Locally Nameless and Locally Named techniques, both use a nominal approach to represent global names. Hence we reuse *atoms* from section 2.1.1 and package them up as a little module. These atoms form our set of global names. This tiny module contains a type for atoms \( \text{Atom} \), an equality test \( _\cong \), and an injective function from natural numbers to atoms:

```haskell
module Data.Atom where

abstract
  Atom : Set
  Atom = N

  _\cong : (x y : Atom) \to Bool
  _\cong = _\congN_

  _^A : N \to Atom
  _^A = \text{id}
```

Since our library supports both de Bruijn indices and the nominal style,
the type \( \text{Name} \) can be used to represent local names. Our type for names is indexed by a world, hence internally, terms are indexed as well. However the manipulated terms being locally closed, the world is always the empty world in the end. Hence we happen to reach a local name, this name inhabits the empty world. Thanks to the function \( \text{Name}_\emptyset\)-elim (based on \( \neg \text{Name}_\emptyset \)), we know that such a case is impossible.

### 6.1.1 Locally closed terms

To illustrate these techniques and how we can use our library to develop these techniques, we use a type for terms like we have done so far. However we do not define the type \( \text{Tm}_\emptyset \) yet (which is not the type \( \text{Tm}_\emptyset \) from section 2.1.1): instead, we assume the following types and data constructors.

\[
\begin{align*}
\text{Tm}_\emptyset &: \text{Set} \\
\text{AbsTm} &: \text{Set} \\
\text{V}_\emptyset &: (x : \text{Atom}) \rightarrow \text{Tm}_\emptyset \\
\text{V}_\emptyset &: (x : \text{Name}_\emptyset) \rightarrow \text{Tm}_\emptyset \\
\lambda &: (\text{abs} : \text{AbsTm}) \rightarrow \text{Tm}_\emptyset \\
\_ \_ &: (t \_u : \text{Tm}_\emptyset) \rightarrow \text{Tm}_\emptyset \\
\text{Let} &: (t : \text{Tm}_\emptyset) \rightarrow (\text{abs} : \text{AbsTm}) \rightarrow \text{Tm}_\emptyset
\end{align*}
\]

In order to deal with the type \( \text{AbsTm} \), the two functions \( \text{openTm} \) and \( \text{closeTm} \) are given to eliminate and introduce values of type \( \text{AbsTm} \).

\[
\begin{align*}
\text{closeTm} &: \text{Atom} \rightarrow \text{Tm}_\emptyset \rightarrow \text{AbsTm} \\
\text{openTm} &: \text{Atom} \rightarrow \text{AbsTm} \rightarrow \text{Tm}_\emptyset
\end{align*}
\]
Generally when writing the function \texttt{openTm}, it is no more difficult to plug a term than it is to plug an atom. This is especially true since the plugged term is locally closed, since no capture can happen. Hence we prefer to define the function \texttt{openSubstTm} for each implementation and define \texttt{openTm} generically.

\[ \texttt{openSubstTm} : \text{Tm}^A \rightarrow \text{AbsTm} \rightarrow \text{Tm}^A \]

\[ \texttt{openTm} : \text{Atom} \rightarrow \text{AbsTm} \rightarrow \text{Tm}^A \]

\[ \texttt{openTm} = \texttt{openSubstTm} \circ \text{V}^A \]

### 6.1.2 Building terms

To build terms easily one can build smart constructors hiding the underlying use of \texttt{closeTm}. Hence we introduce two functions \( \chi' \) and \( \texttt{let}' \) to build \( \lambda \)-abstractions and local definitions in a more natural way. In particular in the case of \( \texttt{let}' \) this is the occasion to put the arguments in the expected order:

\[ \chi' : \text{Atom} \rightarrow \text{Tm}^A \rightarrow \text{Tm}^A \]

\[ \chi' x t = \chi (\text{closeTm} \ x \ t) \]

\[ \texttt{let}' : \text{Atom} \rightarrow \text{Tm}^A \rightarrow \text{Tm}^A \rightarrow \text{Tm}^A \]

\[ \texttt{let}' x t u = \text{Let} \ t (\text{closeTm} \ x \ u) \]

We can now build various terms quite easily:

\[ \texttt{id}^T : \text{Tm}^A \]

\[ \texttt{id}^T = \chi' x (\text{V}^A x) \]

\[ \text{where } x = 0^A \]

\[ \texttt{false}^T : \text{Tm}^A \]

\[ \texttt{false}^T = \chi' x (\chi' x (\text{V}^A x)) \]

\[ \text{where } x = 0^{\chi'} \]

\[ \texttt{true}^T : \text{Tm}^A \]

\[ \texttt{true}^T = \chi' x (\chi' y (\text{V}^A x)) \]

\[ \text{where } x = 0^{\chi'}, y = 1^A \]

\[ \texttt{ap}^T : \text{Tm}^A \]

\[ \texttt{ap}^T = \chi' x (\chi' y (\text{V}^A x \cdot \text{V}^A y)) \]

\[ \text{where } x = 0^A, y = 1^A \]
Opening and closing operations need to deal with local variables. However any other operation could be built with only openTm and closeTm, hence without any knowledge of the local variables. Using openTm and closeTm also has three main limitations: convenience, performance and non-structural recursion. Since all of them apply on most functions over terms we take a concrete example with a function size which tries to count the number of constructors in a term:

\[
\begin{align*}
\text{size} : \text{Tm}^A &\rightarrow \mathbb{N} \\
\text{size} (\text{V}^A \_ &\_ ) = 1 \\
\text{size} (\text{fct} \cdot \text{arg} ) = 1 + \text{size fct} + \text{size arg} \\
\text{size} (\text{\lambda} \text{ abs} ) = 1 + \text{size (openTm (0 A) abs) } \\
\text{size} (\text{Let t abs} ) = 1 + \text{size t} + \text{size (openTm (0 A) abs) } \\
\text{size} (\text{V}^A \_x ) = \text{Name}_\emptyset - \text{elim x}
\end{align*}
\]

**Convenience** While closeTm can be hidden with smart constructors, openTm has to be explicitly used, which hinders pattern-matching. Indeed, without view-patterns (see [Wadler, 1987] for the seminal work on view patterns), pattern-matching has to be stopped at abstractions, in order to call openTm. The deeper the pattern, the worse the trouble. Moreover in this presentation we have to provide a global name to open the abstraction, which often requires an atom supply to give different atoms each time. In the size function we constantly open abstractions with the atom 0 A which is acceptable only because we do not care about the identity of variables in this example.

### 6.1.3 Performances

From a performance point of view openTm and closeTm require to traverse the whole subterm. They thus increase the asymptotic complexity of most algorithms. For a term of size n the asymptotic complexity of openTm and closeTm is naturally between O(n) and O(n*log(n)). To our knowledge the complexity cannot be reduced much without losing properties such as persistence. In Coml [Pottier, 2006] the opening operation lazily performs the required substitution. We describe Coml and connect it to our work in section 6.5.2. For traditional algorithms the cost of opening (and
closing) is amortized but the presence of delayed substitutions makes the worst-case complexity exponential.

Let us look at how performance degrades on some algorithms. For instance an algorithm on a term that is simple enough to not involve the binding structure and that usually has a linear complexity, has a quadratic complexity when using `openTm` and `closeTm`. Algorithms to extract some information such as the size of a term (our function `size`) or the presence of some constructs in a term are of this kind. Algorithms to transform some non-binding constructs such as constant-folding, control-flow rewriting, assertions insertion or suppression, etc. are of this kind as well. Even some algorithms operating on the binding structure would benefit from avoiding `openTm` and `closeTm`. Here are for instance two functions in nominal style to transform back and forth, local `let` bindings into applied λ-abstractions. With our library no run-time cost is incurred and these two operations work in linear time:

```haskell
module Let⇒X where
⟨⟨_⟩⟩ : ∀ {α} → Tm α → Tm α
⟨⟨ λ b t · u ⟩⟩ = Let b ⟨⟨ u ⟩⟩ ⟨⟨ t ⟩⟩
⟨⟨ V x ⟩⟩ = V x
⟨⟨ t · u ⟩⟩ = ⟨⟨ t ⟩⟩ · ⟨⟨ u ⟩⟩
⟨⟨ λ b t ⟩⟩ = λ b ⟨⟨ t ⟩⟩
⟨⟨ Let b t u ⟩⟩ = Let b ⟨⟨ t ⟩⟩ ⟨⟨ u ⟩

module X⇒Let where
⟨⟨_⟩⟩ : ∀ {α} → Tm α → Tm α
⟨⟨ Let b t u ⟩⟩ = X b ⟨⟨ u ⟩⟩ · ⟨⟨ t ⟩⟩
⟨⟨ V x ⟩⟩ = V x
⟨⟨ t · u ⟩⟩ = ⟨⟨ t ⟩⟩ · ⟨⟨ u ⟩⟩
⟨⟨ λ b t ⟩⟩ = λ b ⟨⟨ t ⟩⟩

6.1.4 Non-structural recursion

The third main limitation of these approaches – at least from the point of view of a total language such as Agda – is that `openTm` hinders structural recursion. Structural recursion is a syntactic criterion requiring to make recursive calls only on syntactic subterms of the input. Indeed if `t` is a subterm of a term `u`, `openTm s t` is not a subterm of `u`, preventing any recursive call. Of course we can claim for a better support for this kind of recursion, since `openTm` preserves the `size` of its input.

Our `size` function does not escape the rule and Agda’s termination checker complains by coloring in red two offending recursive calls. In order to workaround this limitation, we give a new parameter to `size` called `fuel`
6.1. DYNAMICALLY STRATIFIED REPRESENTATIONS

of type \( N \), on which occurs the structural recursion. When we hit 0 we have not enough gas to proceed and return a dummy value. If given enough fuel the function behaves correctly. Generally it suffices to pick an upper bound for the fuel parameter. Here a good upper bound would be the size of the term...

```
-- 'fuel-extended' to pass the termination checker
size : (fuel : N) \rightarrow \text{Tm}^A \rightarrow N
size (suc n) (V^A x) = 1
size (suc n) (fct \cdot arg) = 1 + size n fct + size n arg
size (suc n) (\times abs) = 1 + size n (\text{openTm} (0^A) abs)
size (suc n) (\text{Let t abs}) = 1 + size n t + size n (\text{openTm} (0^A) abs)
size (suc n) (V^N x) = \text{Name}^0\text{-elim x}
size 0 _ = 0 -- dummy
```

6.1.5 Free atoms using openTm

A more interesting example is to compute the list of free variables, more precisely of free atoms. In order to define it independently of the representation of local name abstractions, we use openTm. Since the identity of atoms matters here, we take an atom supply as an argument to open abstractions with atoms that are fresh for the current context. Indeed there is no need to thread the atom supply here since we remove the atom afterward. A fuel argument is added to pass the termination checker. These two parameters would benefit from being hidden as a monad, at least for conveniently using and combining these functions. The function \( \text{fa} \) uses the function \( \text{rm}^A \) which was defined in section 2.1.1.

```
module FreeAtoms where

fa : (fuel atomSupply : N) \rightarrow \text{Tm}^A \rightarrow \text{List Atom}
fa (suc n) (V^N x) = \text{Name}^0\text{-elim x}
fa (suc n) (V^A x) = [ x ]
fa (suc n) s (fct \cdot arg) = fa n s fct ++ fa n s arg
fa (suc n) s (\times abs)
  = \text{rm}^A (s^A) (fa n (1 + s) (\text{openTm} (s^A) abs))
fa (suc n) s (\text{Let t abs})
  = fa n s t ++
  \text{rm}^A (s^A) (fa n (1 + s) (\text{openTm} (s^A) abs))
fa 0 _ _ = [] -- dummy
```
6.1.6 Common parts of the internal representation

The type $Tm^A$ is for locally closed terms. This type is based on a more general type for terms with potential free local names. This type is called $PreTm$ and is indexed by a world. The only implementation specific part is the representation of name abstractions. The type $AbsPreTm$ represents a name abstraction and can be implemented in various ways.

\[
AbsPreTm : \text{World} \rightarrow \text{Set}
\]

\[
data \ PreTm \alpha : \text{Set where}
\]

\[
V^N : (x : \text{Name} \alpha) \rightarrow PreTm \alpha
\]

\[
V^A : (x : \text{Atom}) \rightarrow PreTm \alpha
\]

\[
\cdot \cdot : (t u : PreTm \alpha) \rightarrow PreTm \alpha
\]

\[
\times : (t : AbsPreTm \alpha) \rightarrow PreTm \alpha
\]

\[
\text{Let} : (t : PreTm \alpha) (u : AbsPreTm \alpha) \rightarrow PreTm \alpha
\]

AbsPreTm = \{! implementation specific !\}

Once the types $PreTm$ and $AbsPreTm$ are defined, defining the locally closed variants amounts to choose the empty world.

-- Locally closed terms
\[
Tm^A : \text{Set}
\]

\[
Tm^A = PreTm ()
\]

-- Locally closed abstracted terms
\[
AbsTm : \text{Set}
\]

\[
AbsTm = AbsPreTm ()
\]

6.1.7 Locally Nameless

We can now focus on specific details of local variables. We start with Locally Nameless [Charguéraud, 2011, Aydemir et al., 2008]. To do so we only have to choose the representation of name abstractions. We make use of the type $SynAbs^D$ defined in Figure 6.1:

\[
AbsPreTm = SynAbs^D PreTm
\]

Substituting definitions for $AbsPreTm$ and $SynAbs^D$ in the definition of $PreTm$ yields the type $Tm^D$ with an extra constructor for atoms:
6.1. DYNAMICALLY STRATIFIED REPRESENTATIONS

\[
\text{SynAbs}^N \quad F \alpha = \exists[b](F(b \triangleleft \alpha)) \\
\text{SynAbs}^D \quad F \alpha = F(\alpha \uparrow 1) \\
\text{SynAbs}^L \quad F \ b \alpha = F(suc^N b)(b \triangleleft \alpha) \\
\text{SemAbs} \quad F \alpha = \forall \beta \rightarrow \alpha \subseteq \beta \rightarrow F\beta \\
\text{SemAbs}^+ \quad F \alpha = \forall \{k\} \rightarrow (\alpha +^N k) \subseteq \beta \rightarrow F\beta \\
\text{SynAbs}^# \quad F \alpha = \exists[b](b \# \times F(b \triangleleft \alpha)) \\
\text{SemAbs}^+ \quad W \ F \alpha = \forall \beta \rightarrow \alpha \subseteq \beta \rightarrow F\beta \\
\text{SynAbs}^# \quad N \ F \alpha = \exists[b](F(b \triangleleft \alpha)) \\
\text{SynAbs}^# \quad \exists[b](b \triangleleft \alpha) \\
\sim \exists[b](b \triangleleft \alpha) \\
\sim \exists[b](b \triangleleft \alpha) \\
\sim \exists[b](b \triangleleft \alpha) \\
\sim \exists[b](b \triangleleft \alpha)
\]

Figure 6.1: Various forms of name abstraction

-- Once AbsPreTm and SynAbs^D are expanded:

\[
data \text{PreTm} \alpha : \text{Set where} \\
\forall^N : (x \text{: Name } \alpha) \rightarrow \text{PreTm } \alpha \\
\forall^A : (x \text{: Atom}) \rightarrow \text{PreTm } \alpha \\
\cdot \_ : (t \text{: PreTm } \alpha) \rightarrow \text{PreTm } \alpha \\
\chi : (t \text{: PreTm } (\alpha \uparrow 1)) \rightarrow \text{PreTm } \alpha \\
\text{Let : } (t \text{: PreTm } \alpha) (u \text{: PreTm } (\alpha \uparrow 1)) \rightarrow \text{PreTm } \alpha
\]

We then define a module TraversePreTm (code omitted) like in section 5.3.4 to generically derive various operations including the coercion operation, and the substitution operation:

-- These two functions are derived from TraversePreTm

\[
\text{coercePreTm} : \forall \{\alpha \beta\} \rightarrow \alpha \subseteq \beta \rightarrow \text{PreTm } \alpha \rightarrow \text{PreTm } \beta \\
\text{substPreTm} : \forall \{\alpha \beta\} \rightarrow (\text{Name } \alpha \rightarrow \text{PreTm } \beta) \\
\rightarrow \text{PreTm } \alpha \rightarrow \text{PreTm } \beta
\]

We can finally define openSubstTm and closeTm. The function openSubstTm is a simple use of substitution on terms using the function substPreTm. The argument to substPreTm replaces 0 by t using the function exportWith:

\[
\text{openSubstTm} : \text{Tm}^A \rightarrow \text{AbsTm} \rightarrow \text{Tm}^A \\
\text{openSubstTm} t = \text{substPreTm} (\text{exportWith } t (\text{Name-elim } \emptyset +^1 \subseteq \emptyset))
\]

The function closeTm is essentially the combination of a coercion from the empty world to the world \(\emptyset \uparrow 1\) and a replace operation of an atom by a name referring to the newly introduced binder at the root. To make this replacing operation we simply carry on a name which we initialize with \(0^N\) and increment when going down under the abstractions with \(suc^N\). While we could have fused these operations we did not for the clarity of the code.
closeTm : Atom → Tm^A → AbsTm

closeTm a t = ! (0 ^A) (coerce(PreTm t) t) where

-- "'! y t'" replaces "'a'" by "'y'" in "'t'"

! : ∀ {α} → Name α → PreTm α → PreTm α

! y (V^A x) = if x ==^A a then V^B y else V^A x

! y (t · u) = ! y t · ! y u

! y (x t) = x (! (suc^B y) t)

! y (Let t u) = Let (! y t) (! (suc^B y) u)

6.1.8 Locally Named

Local names bindings can be changed from de Bruijn indices to a nominal style by updating \textit{AbsPreTm}. We use \textit{SynAbs^B} from section 3.4 and Figure 6.1:

\text{AbsPreTm} = \text{SynAbs^B PreTm}

The resulting type \textit{PreTm} is similar to the type \textit{Term} from section 3.4 and to the type \textit{Tm^A} from section 2.1.1. However, name-abstractions are packed into pairs and there is an extra constructor for atoms.

As usual we define a traversal function along the lines of section 3.2 with an extra argument to deal with the constructor \textit{V^A}:

\text{TraversePreTm.tr} :

∀ {E} {Env} (E-app : Applicative E)

{trKit} {trAtm} {α β} → Env α β → Atom → E (PreTm β)

{α β} → Env α β → PreTm α → E (PreTm β)

From this traversal we obtain various operations including substitution:

\text{substPreTm} : ∀ {α β} → Supply β → (Name α → PreTm β)

→ PreTm α → PreTm β

From the function \text{substPreTm} we quickly get the function \text{openSubstTm}:

\text{openSubstTm} : Tm^A → AbsTm → Tm^A

openSubstTm t (., u) = substPreTm t (0 ^B) (exportWith t Name0-elim) u

The function \text{closeTm} is a bit more challenging. We define a new traversal kit called \textit{renameKit^+} on a new environment type \textit{SubstEnv^+}. This
environment type packages a renaming environment and an inclusion witness to maintain the fact that we freshened the output term and hence can import anything from the root output world.

\[
\text{record } \text{SubstEnv} \subseteq \text{Res} \beta_0 \alpha \beta : \text{Set where}
\]
\[
\text{constructor } . .
\]
\[
\text{field}
\]
\[
\text{ren} : \text{SubstEnv} \text{Res} \alpha \beta
\]
\[
\text{pf} : \beta_0 \subseteq \beta
\]
\[
\text{open } \text{SubstEnv ren public}
\]

This traversal kit behaves such as the renaming kit (renameKit) on page 65:

\[
\text{renameKit} \subseteq : \forall \beta_0 \rightarrow \text{TrKit} (\text{SubstEnv} \subseteq \text{Name} \beta_0) \text{Name}
\]
\[
\text{renameKit} \subseteq \beta_0 = \text{mk trName trBinder extEnv}
\]
\[
\text{where}
\]
\[
\text{Env} = \text{SubstEnv} \subseteq \text{Name} \beta_0
\]
\[
\text{open } \text{SubstEnv} \subseteq
\]
\[
\text{extEnv} : \forall \{\alpha \beta\} \ b (\Delta : \text{Env} \alpha \beta) \rightarrow \text{Env} (b \triangleleft \alpha) (\text{seed}^\beta \Delta \triangleleft \beta)
\]
\[
\text{extEnv} b (\text{ren} , \text{pf}) =
\]
\[
\text{(TrKit.}\text{extEnv renameKit b ren} ,
\]
\[
\subseteq - \text{trans pf (SubstEnv.seed} \subseteq \text{ren}))
\]

Finally closeTm is defined using the traversal function TraversePreTm.tr, the kit renameKit+\subseteq, and the special behavior on atoms defined in the local function trAtm:

\[
\text{closeTm} : \text{Atom} \rightarrow \text{Tm}^A \rightarrow \text{AbsTm}
\]
\[
\text{closeTm} a t = 0^B , \text{tr (renameEnv}^\subseteq 1 , \subseteq - \text{refl}) t \text{where}
\]
\[
\beta_0 = .
\]
\[
\text{trAtm} : \forall \{\alpha \beta\} \rightarrow \text{SubstEnv} \subseteq \text{Name} \beta_0 \alpha \beta \rightarrow \text{Atom} \rightarrow \text{PreTm} \beta
\]
\[
\text{trAtm} \Delta a' = \text{if } a =^A a' \text{ then } V^H (\text{coerce}^H (\text{SubstEnv} \subseteq . \text{pf} \ \Delta) (0^W))
\]
\[
\text{else } V^A a'
\]
\[
\text{kit} = \text{mapKit id } V^H (\text{renameKit} \subseteq \beta_0)
\]
\[
\text{tr} = \text{TraversePreTm.tr id-app kit trAtm}
\]

While we have a construction for Locally Named terms, this is not yet exactly the approach described by Sato and Pollak [Pollack et al., 2011, Sato and Pollack, 2010]. Indeed we have not yet integrated the height function which yields a different function to close terms. This means that we do not
get the nice properties either, for instance our Locally Named representation is not canonical. However the canonical representation is less crucial in our setting since our interface prevents from observing these representation details.

6.1.9 When does this stratified technique pay off?

So far we described these “dynamically stratified representations”, explained how we build them on top of our library, and explained the limitations of an exclusive usage of open/close functions. We claim that this technique can be of great effect when the static discipline of our library becomes too heavy. Contrary to most of the Locally Nameless implementations we argue that the name-abstraction should not be an abstract type. In particular with our library, no safety is lost by keeping name-abstraction concrete since we have precise worlds. Moreover, as we have shown, adding atoms to represent external names is the only change we have to make beforehand to our data type to support this technique.

Generalizing from atoms to arbitrary constants   We advise users of our library to have a case for constants in their representation of terms for instance. These “constants” could be numbers, atoms, or a type parameter to be chosen afterward. We illustrate with two situations how this can be used effectively.

In the first situation, the client builds a function \( f \) which requires an extra environment argument to work on open terms. In the second situation the client is only able to define a function \( f-c \) for closed terms. One can often reduce the first situation to the second if we have an environment for the empty world. In these situations we end up with a function working only on closed terms. However if we pick the type of constants to be atoms, we have a function \( f-lc \) working on locally closed terms.

```plaintext
-- Terms parameterized by constants
Tm : Set → World → Set

-- We suppose that producing an initial environment
-- for arbitrary worlds is difficult.
Env : World → World → Set
```
6.1. DYNAMICALLY STRATIFIED REPRESENTATIONS

-- We suppose the environment for empty worlds
to be easy to produce.
\( \epsilon : Env()() \)

-- Situation 1: A function on open terms
\( f : \forall \{\alpha, \beta \text{ Cst}\} \to Env\alpha\beta \to Tm\text{ Cst }\alpha \to Tm\text{ Cst }\beta \)

-- Situation 2: Like \( f \) but works on closed terms
\( f-c : \forall \{\text{ Cst}\} \to Tm\text{ Cst }\emptyset \to Tm\text{ Cst }\emptyset \)
\( f-c = f \; \epsilon \)

-- Locally closed terms
\( \text{LCTm} = Tm\text{ Atom }\emptyset \)

-- Like \( f \) but on locally closed terms
\( f-\text{lC} : \text{LCTm} \to \text{LCTm} \)
\( f-\text{lC} = f-c \)

As we can see with the definitions of \( f-c \) and \( f-\text{lC} \) not much happened.
In this example we are indeed supposing that nothing is done on constants
and that this is correct to treat them parametrically. In this case what has
been done is simply to tell the user of the function to convert all the free
variables into atoms before calling the function.

We can spare the conversion to the user and do it ourselves. To do so,
we show that given enough traversal functions on terms the two following
types are equivalent:

\( \forall \{\text{ Cst}\} \to Tm\text{ Cst }\emptyset \to Tm\text{ Cst }\emptyset \)
\( \cong \)
\( \forall \{\alpha \text{ Cst}\} \to Tm\text{ Cst }\alpha \to Tm\text{ Cst }\alpha \)

We focus on the non-immediate direction, that is going from the first
type to the second. In this situation we can even define this transformation
as a higher-order function. Here we do not use atoms but keep names, and
we preserve the original constants as well. We call the function \( f \) with the
type \( \text{Name }\alpha \uplus \text{Cst} \) for constants, where \( \text{Cst} \) is the type of original constants
and \( \alpha \) is the world of free variables. Once the constants are preserved using
the \( \text{bindTm} \) function, the free variables are turned into constants as well
using the function \( \text{substTm} \). Then the function \( f \) operates on the locally
closed term. This yields a locally closed term as well that we coerce to
the world \( \alpha \). Finally we restore the original constants and free variables
using the function \( \text{bindTm} \) and the eliminator of sums: \([,] \). The following
function \( \text{transform} \) is in a parameterized module \( M \) such that it only depends
on our library:

```haskell
module M
  (Tm : Set → World → Set)
  (cst : ∀ {α Cst} → Cst → Tm Cst α)
  (var : ∀ {α Cst} → Name α → Tm Cst α)
  (substTm : ∀ {α Cst} → (Name α → Tm Cst ∅) → Tm Cst α → Tm Cst ∅)
  (bindTm : ∀ {α A B} → (A → Tm B α) → Tm A α → Tm B α)
  (coerce∅Tm : ∀ {α Cst} → Tm Cst ∅ → Tm Cst α)
  (f : ∀ {Cst} → Tm Cst ∅ → Tm Cst ∅)
where

transform : ∀ {α Cst} → Tm Cst α → Tm Cst α
transform = bindTm [ cst , var ] -- untag constants and variables
  ◦ coerce∅Tm -- closed terms inhabit any world
  ◦ f -- operate on locally closed terms
  ◦ substTm (cst ◦ inj2) -- tag variables as constants by 2
  ◦ bindTm (cst ◦ inj1) -- tag original constants by 1
```

We can see open and close functions like a way to move the border between the bound names and free names. When we do not call the open function and directly go under a name abstraction, it is as if we implicitly moved the border. This implicit move is one of the main sources of bugs in programs dealing with names and binders. In our system the border is reflected in the types using the worlds. Hence this distinction incurs no cost at run-time and still prevents mistakes caused by confusing bound and free names.

We have shown how to build dynamically stratified representations on top of our library. We have reused our technique to represent binders and local names, but used an atom type for global names. We have built both a Locally Nameless implementation and a basic Locally Named implementation including the traditional open and close functions. These techniques have shown their advantages as a tool for meta-theory, to reason about programming languages. We have shown the limitations that we think these techniques have for programming. We think these techniques are akin to dynamic typing. Indeed the tagging of names as local or global helps write functions without considering the free variables of the input. We have then shown how we can recover this benefit by having terms parameterized by constants. As soon as constants are handled parametrically we can transform any function over closed terms to a function on open terms. However
we recognize these dynamically stratified approaches may be simpler to use than our approach and still provide more safety than the bare approaches.

6.2 de Bruijn levels

Let us briefly mention another representation called “de Bruijn levels”. This is another nameless representation different from de Bruijn indices. λ-abstractions are implicitly labeled starting at 0 from the root, and variable occurrences simply refer to these labels. De Bruijn levels are actually very close to a nominal presentation since every reference to a given binder is represented identically. However, binders are not freely chosen, as in nominal style, but dictated by the position of the term starting from the root. We can accommodate this style by indexing terms by the next available binder:

data Tm^L s α : Set where
  V : Name α → Tm^L s α
  ·· : (t u : Tm^L s α) → Tm^L s α
  λ : Tm^L (suc^B s) (s < α) → Tm^L s α
  Let : Tm^L s α → Tm^L (suc^B s) (s < α) → Tm^L s α

The type Tm^L is a variant of our type Tm which is not only indexed by a world but by a binder s as well. This binder s tells how far we are from “the root”. This binder is carried down by a constructor such as ··. At a λ-abstraction, the binder index is used and becomes bound in the subterm; moreover, the index is incremented in the subterm. Most functions work as in nominal style: for instance, the function fv requires no fundamental changes. The extra cost is this new index appearing in the types of terms. The benefit is that given an initial binder index, the representation is canonical.

6.2.1 Term comparison

Comparing terms in de Bruijn level style is no different than in nominal style. A name-comparator is carried down and extended with the same function extendNameCmp. In the end, the resulting function makes no restriction on the seeds of the input terms. This emphasises again that our comparison function makes no attempt to compare binders between the two arguments. Bound variable are compared positionally. Here is the signature for the function cmpTm^L:

cmpTm^L : ∀ {α β s_1 s_2} → |Cmp| Name α β
         → (Tm^L s_1 α → Tm^L s_2 β → Bool)
However one may want to exploit the canonical structure of our repre-
sentation for terms. We have already done so for de Bruijn indices with
the function $eq\text{Tm}^D$ in section 5.3.5. When both terms starts with the same
binder index and world, then their types stays in synch. When reaching
variable occurrences the equality test on names can be applied [Pouillard,
2011a].

$$\_==\text{Tm}_L^- : \forall \{\alpha s\} \to \text{Tm}^L s \alpha \to \text{Tm}^L s \alpha \to \text{Bool}$$

$$V x_1 ==\text{Tm}^L V x_2 = x_1 ==\text{LL} x_2$$

$$(t_1 \cdot u_1) ==\text{Tm}^L (t_2 \cdot u_2) = t_1 ==\text{Tm}^L t_2 \land u_1 ==\text{Tm}^L u_2$$

$$\land t_1 ==\text{Tm}^L \land t_2 = t_1 ==\text{Tm}^L t_2$$

$$\text{Let} t_1 u_1 ==\text{Tm}^L \text{Let} t_2 u_2 = t_1 ==\text{Tm}^L t_2 \land u_1 ==\text{Tm}^L u_2$$

$$\_ ==\text{Tm}^L _ = false$$

De Bruijn level operations are similar to nominal operations. A first
difference is that binding constructs do not have to hold a binder since the
binder is fixed by the index. This gives a nameless flavor to this presentation
but our typed presentation shows where the binders have gone: in the types.

To illustrate how binders moved out of the terms we can look at snippets
of functions with all the arguments made explicit:

$$f^R : \forall \{\alpha\} \to \text{Tm} \alpha \to \ldots$$

$$f^R \{\alpha\} (\land b t) = \ldots$$

$$f^L : \forall \{b \alpha\} \to \text{Tm}^L b \alpha \to \ldots$$

$$f^L \{b\} \{\alpha\} (\land t) = \ldots$$

The first snippet is in nominal style and the binder $b$ is found in the
term. The second snippet uses de Bruijn levels and the binder $b$ comes as
a separate (implicit) argument. In the end we have the same data in both
snippets. We can see this as a good news, as it helps recover the information
lost by this nameless representation.

For instance functions such as $fv$ and $coerce\text{Tm}$ require almost no change
to be adapted from nominal to de Bruijn levels.

### 6.2.2 Kits and traversals

We develop kits and traversals in a way similar to section 3.2. Since our
terms are now indexed by a binder as well, environments are indexed by two
worlds and two binders.

$$\text{EnvType}^L : \text{Set}_1$$

$$\text{EnvType}^L = (s_1 s_2 : \text{Binder}) (\alpha \beta : \text{World}) \to \text{Set}$$
Kits are made of only two functions \texttt{trName} and \texttt{extEnv}. There is no need for an equivalent of the function \texttt{trBinder} since binders now appear in indices and can thus be controlled through the environment type.

\[
\text{TrName} : (Env : \text{EnvType}) \rightarrow (Res : \text{Binder} \rightarrow \text{World} \rightarrow \text{Set}) \rightarrow \text{Set}
\]
\[
\text{ExtEnv} : (Env : \text{EnvType}) \rightarrow \text{Set}
\]

\[
\begin{align*}
\text{TrName} & = \forall \{s_1 s_2 \alpha \beta\} \rightarrow \text{Env} s_1 s_2 \alpha \beta \\
& \rightarrow \text{Name} \alpha \rightarrow \text{Res} s_2 \beta
\end{align*}
\]

\[
\begin{align*}
\text{ExtEnv} & = \forall \{s_1 s_2 \alpha \beta\} \rightarrow \text{Env} s_1 s_2 \alpha \beta \\
& \rightarrow \text{Env} (\text{suc}^B s_1) (\text{suc}^B s_2) (s_1 < \alpha) (s_2 < \beta)
\end{align*}
\]

record \texttt{TrKit} (Env : \text{EnvType}) \\
where \\
\text{constructor mk} \\
\text{field} \\
\text{trName} : \text{TrName} Env Res \\
\text{extEnv} : \text{ExtEnv} Env

We have several traversal functions making use of a kit. We give only the most general of them. As in section 3.2 we abstract over an applicative functor, and the kit’s result type is a term. This one suffices to derive all the functions presented in the following:

\[
\text{module TraverseATm} \\
\{E\} (E-app : \text{Applicative} E) \\
\{Env\} (kit : \text{TrKit} Env \rightarrow (\lambda s \alpha \rightarrow E (\text{Tm} s \alpha)))
\]

\[
\begin{align*}
\text{trTm} & = \forall \{\alpha \beta s_1 s_2\} \rightarrow \text{Tm} s_1 s_2 \alpha \beta \\
& \rightarrow E (\text{Tm} s_2 \beta)
\end{align*}
\]

\[
\begin{align*}
\text{trTm} & = \text{trName} x \\
\text{trTm} (t \cdot u) & = \text{pure } \_ \_ \cdot \text{trTm} t \odot \text{trTm} u \\
\text{trTm} (\check{x}) & = \text{pure } \check{x} \odot \text{trTm} (\text{extEnv} \Delta) t \\
\text{trTm} (\text{Let } t u) & = \text{pure Let } \odot \text{trTm} t \odot \text{trTm} (\text{extEnv} \Delta) u
\end{align*}
\]

The equivalent of \texttt{SubstEnv} is called \texttt{SubstEnv}. This one does not require a \texttt{Supply} field, a fresh-for proof suffices. The \texttt{RenameEnv} is a specialization to functions returning names.
record SubstEnv\(^L\) Res\((s_1 \ s_2 : \text{Binder}) \ (\alpha \ \beta : \text{World})\) : Set where
  constructor \_\_\_
  field
  trName\(^L\) : Name \(\alpha \rightarrow \text{Res} \ s_2 \beta\)
  \(s_2 \# \beta \quad : \ s_2 \# \beta\)

\(\text{RenameEnv}^L = \text{SubstEnv}^L \ (\text{const \ Name})\)

\(\text{renameKit}^L : \text{TrKit}^L \ \text{RenameEnv}^L \ (\text{const \ Name})\)

6.2.3 Derived functions

Along the lines of section 3.2, the kit \(\text{renameKit}^L\) is extended to a kit \(\text{renameAKit}^L\) which supports an effectful application. Like before, from these kits we derive several functions. Functions like \(\text{renameTm}^L\), \(\text{renameTm}^L A\), \(\text{renameTm}^L ?\), \(\text{closeTm}^L\), and \(\text{substTm}^L\) are built like their analog from section 3.2. The name supply argument is now just a fresh-for proof since the seed appears in the index. Here are the type signatures for these functions:

\(\text{renameTm}^L : \forall \ \{\alpha \ \beta \ s_1 \ s_2\} \rightarrow s_2 \# \beta \rightarrow (\text{Name} \ \alpha \rightarrow \text{Name} \ \beta)\)

\(\rightarrow \text{Tm}^L \ s_1 \ \alpha \rightarrow \text{Tm}^L \ s_2 \beta\)

\(\text{renameTm}^L A : \forall \ \{E\} \ (E\text{-app} : \text{Applicative} \ E)\)

\(\{\alpha \ \beta \ s_1 \ s_2\} \rightarrow s_2 \# \beta \rightarrow (\text{Name} \ \alpha \rightarrow E \ (\text{Name} \ \beta))\)

\(\rightarrow \text{Tm}^L \ s_1 \ \alpha \rightarrow E \ (\text{Tm}^L \ s_2 \beta)\)

\(\text{renameTm}^L ? : \forall \ \{\alpha \ \beta \ s_1 \ s_2\} \rightarrow s_2 \# \beta \rightarrow (\text{Name} \ \alpha \rightarrow ? \ \text{Name} \ \beta)\)

\(\rightarrow \text{Tm}^L \ s_1 \ \alpha \rightarrow ? \ (\text{Tm}^L \ s_2 \beta)\)

\(\text{closeTm}^L ? : \forall \ \{s \ \alpha\} \rightarrow \text{Tm}^L \ s \ \alpha \rightarrow ? \ \text{Tm}^L \ s \ \emptyset\)

\(\text{substTm}^L : \forall \ \{\alpha \ \beta \ s \ s_2\} \rightarrow s_2 \# \beta \rightarrow (\text{Name} \ \alpha \rightarrow \text{Tm}^L \ s_2 \beta)\)

\(\rightarrow (\text{Tm}^L \ s \ \alpha \rightarrow \text{Tm}^L \ s_2 \beta)\)

We then lift addition and subtraction from names to terms using the function \(\text{renameTm}^L\). The resulting functions get interesting types. In particular the input seed is disconnected from the input seed and this these functions enables to re-level the terms:
6.2. DE BRUIJN LEVELS

protectedAddTm : ∀ {α s₁ s₂} k → s₂ # (α +^W k) → Tm^L s₁ α → Tm^L s₂ (α +^W k)
protectedAddTm k pf = renameTm^L pf (add^B k)

protectedSubtractTm : ∀ {α s₁ s₂} k → s₂ # α → Tm^L s₁ (α +^W k) → Tm^L s₂ α
protectedSubtractTm k pf = renameTm^L pf (subtract^B k)

6.2.4 New inclusion rules

In order to tightly integrate de Bruijn levels, and more generally to mix nominal binders and \(+1\) on worlds, we introduce two new inclusion rules. These two rules state that \(+1\) distributes over \(\llhd\):

\[
\subseteq\text{-dist}++\llhd : \forall \{α b\} → (b \llhd α) +^W k \subseteq (b +^B k) \llhd (α +^W k)
\]

\[
\subseteq\text{-dist}=-\llhd zero = \subseteq\text{-refl}
\]

\[
\subseteq\text{-dist}=-\llhd (\text{succ } n) = \subseteq\text{-trans}(\subseteq\text{-cong}+1 (\subseteq\text{-dist}=-\llhd n))
\]

\[
\subseteq\text{-dist}=-\llhd zero = \subseteq\text{-refl}
\]

\[
\subseteq\text{-dist}=-\llhd (\text{succ } n) = \subseteq\text{-trans}(\subseteq\text{-dist}=-\llhd n)
\]

6.2.5 Addition and subtraction kits

The add kit (Add^L.kit) enables to add a constant to all the names and binders of a given traversable term. The environment of this kit is made of two proofs, one on worlds the other on binders. This environment could hence be removed by an optimizing compiler. Once compiled the resulting function is not hindered by the safe handling of names and binders.

module Add^L k where

Env^L : EnvType^L

Env^L b₁ b₂ α β = (α +^W k) \subseteq β \times (b₁ +^B k) \equiv b₂
\[ \text{trName}^L : \text{TrName}^L \text{Env}^L (\text{const Name}) \]
\[ \text{trName}^L (pf, \_ ) = \text{coerce}^N pf \circ \text{add}^N k \]

\[ \text{kit}^L : \text{TrKit}^L \text{Env}^L (\text{const Name}) \]
\[ \text{kit}^L = \text{mk trName}^L \{! \text{proof omitted}! \} \]

We then briefly mention a generalization of the previous kit which allows not only addition but subtraction as well. This kit works similarly and we just show the environment type and the signature of the function on terms:

\[ \text{AddSubtractEnv}^L s_1 s_2 \alpha \beta = (s_1 +^B k_1) \equiv (s_2 +^B k_2) \times (\alpha +^W k_1) \subseteq (\beta +^W k_2) \]

\[ \text{addSubtractTm}^L : \forall k_1 k_2 \]
\[ \{ \alpha \beta \} \rightarrow (s_1 +^B k_1) \equiv (s_2 +^B k_2) \rightarrow (\alpha +^W k_1) \subseteq (\beta +^W k_2) \rightarrow \text{Tm}^L s_1 \alpha \rightarrow \text{Tm}^L s_2 \beta \]

From this general operation \text{addSubtractTm}^L we derive several operations. We can coerce terms, add a constant, subtract a constant, change the seed index of a closed term, and combinations of those.

\[ \text{coerceTm}^L : \forall \{ s \alpha \beta \} \rightarrow \alpha \subseteq \beta \rightarrow \text{Tm}^L s \alpha \rightarrow \text{Tm}^N s \beta \]
\[ \text{addTm}^L : \forall \{ \alpha s \} k \rightarrow \text{Tm}^L s \alpha \rightarrow \text{Tm}^L (s +^B k) (\alpha +^W k) \]
\[ \text{subtractTm}^L : \forall \{ \alpha s \} k \rightarrow \text{Tm}^L (s +^B k) (\alpha +^W k) \rightarrow \text{Tm}^L s \alpha \]
\[ \text{rerootTm}^L : \forall \{ \alpha \} k_1 k_2 \rightarrow \text{Tm}^L (k_1 +^B) \emptyset \rightarrow \text{Tm}^L (k_2 +^B) \alpha \]

6.2.6 Conversion with nominal terms

Converting de Bruijn level terms to nominal could not be simpler. The code [Pouillard, 2011a] is a simple recursive copy where Agda can even infer the binders to choose to build the nominal terms. When converting, we are simply moving a static information to a dynamic place. When reaching a binding construct the binder is known to be the index of the term. This binder also a valid binder to be used to build the resulting binding construct in nominal style. Here is the conversion function we obtain:

\[ \text{module Tm}^L \Rightarrow \text{Tm}^N \text{ where} \]
\[ \langle \_ \rangle : \forall \{ \alpha s \} \rightarrow \text{Tm}^L s \alpha \rightarrow \text{Tm}^N \alpha \]
\[ \langle V x \rangle = V x \]
\[ \langle \lambda t \rangle = \lambda _\_ \langle t \rangle \]
\[ \langle t \cdot u \rangle = \langle t \rangle \cdot \langle u \rangle \]
\[ \langle \text{Let } t u \rangle = \lambda _\_ \langle u \rangle \cdot \langle t \rangle \]
6.3. LINKS: BINDERS AS WORLD RELATIONS

The conversion from nominal to de Bruijn levels is a bit more complicated. Indeed nominal bound variables have to be renamed to follow the discipline of levels. We implement this function by first writing a traverse function from nominal terms to de Bruijn level terms. Then we make use of the renaming kit with little changes. Here are the functions we obtain:

\[
\text{renameTm}^L \Rightarrow \text{Tm}^N : \forall \{\alpha \beta s\} \rightarrow s \# \beta \rightarrow (\text{Name} \alpha \rightarrow \text{Name} \beta) \\
\rightarrow (\text{Tm}^N \alpha \rightarrow \text{Tm}^L s \beta)
\]

\[
\text{renameTm}^L \Rightarrow \text{Tm}^N = \{! \text{ code omitted } !\}
\]

\[
\text{convTm}^N(\emptyset) \Rightarrow \text{Tm}^L : \forall \{s \beta\} \rightarrow s \# \beta \rightarrow \text{Tm}^N(\emptyset) \rightarrow \text{Tm}^L s \beta
\]

\[
\text{convTm}^N(\emptyset) \Rightarrow \text{Tm}^L \#s \beta = \text{renameTm}^L \Rightarrow \text{Tm}^N \#s \beta \text{Name}(\emptyset)\text{-elim}
\]

\[
\text{convTm}^N(\emptyset) \Rightarrow \text{Tm}^L(\emptyset) : \forall s \rightarrow \text{Tm}^N(\emptyset) \rightarrow \text{Tm}^L s \emptyset
\]

\[
\text{convTm}^N(\emptyset) \Rightarrow \text{Tm}^L(\emptyset) s = \text{convTm}^N(\emptyset) \Rightarrow \text{Tm}^L(s \#(\emptyset))
\]

Conclusion  We have shown how de Bruijn levels can be implemented using our library. Our types are now indexed by a world and a binder. This binder is a seed for a binder supply. This seed is to be used for the binder of the next binding construct. For the subterms of binding constructs we increment the seed and extend the world in a nominal style using _\ll. We have shown how close this style was from the nominal style and have derived operations on terms by applying techniques developed for the nominal style. This style also reuses tools we built for de Bruijn indices such as additions on worlds and names (_+^X_ and _↑^\ell_). The extra index can be cumbersome to track, but can also help, as in the equality test on terms. We took advantage of the representation to build a faster equality test and a faster addition function.

6.3 Links: Binders as World Relations

So far with our library, name-abstraction induced a particular form of world for the subterm. In nominal style, we use _\ll_ and in de Bruijn indices style we use _↑^1_. These forms of worlds induce the use of dependent types in nominal style and computation on types in de Bruijn indices style. In nominal style, dependent types occur since binders appear in worlds. In de Bruijn computation on the level of worlds (hence types) occur with the use of arbitrary shifts and additions on worlds _α ↑^k_ and _α ↑^\ell_. In our work of 2010 [Pouillard and Pottier, 2010], the interface relies only on world-polymorphism and since world are erased it avoids dependent types. After our work of 2010 we put aside the idea of links and have developed the
interface presented so far using dependent types leading to a more precise and concrete interface.

In this section we come back to a link based interface. We start by describing an interface for binding-links or simply links. A link is a type parameterized by two worlds which supports the following three operations: \texttt{weaken}, \texttt{strengthen?}, and \texttt{nameOf}. The first parameter of the link is called the outer world and the second the inner world. A link can be seen as a binder $b$ plus a relation between the inner and the outer world. The outer world describes the binders before the introduction of $b$ and the inner world describes the binders after its introduction. The first operation moves a name from the outer world to the inner world, it is a weakening. The second operation tries to move a name from the inner world to the outer world but may fail if we try to move the name being bound by the binding-link. The third operation reveals the name being bound, which belongs to the inner world. In AGDA we have the following record:

$$\begin{align*}
\text{record } \text{Link} \ (\_ \rightarrow \_ : (\alpha \beta : \text{World}) \rightarrow \text{Set}) : \text{Set} \text{ where }
\text{constructor } \text{mk}
\text{ field}
\phantom{\text{weaken}} & : \forall \ (\alpha \beta) \rightarrow \alpha \Rightarrow \beta \rightarrow \text{Name } \alpha \rightarrow \text{Name } \beta \\
\phantom{\text{strengthen?}} & : \forall \ (\alpha \beta) \rightarrow \alpha \Rightarrow \beta \rightarrow \text{Name } \beta \rightarrow ? \text{Name } \alpha \\
\phantom{\text{nameOf}} & : \forall \ (\alpha \beta) \rightarrow \alpha \Rightarrow \beta \rightarrow \text{Name } \beta
\end{align*}$$

\subsection{6.3.1 Terms and examples}

Using links, one can define data types, like our type \texttt{Tm} for terms. As usual the interesting cases are the binding constructs. In particular in the construct \texttt{Let} we see how the use of inner and outer worlds control the defined scopes.

$$\begin{align*}
\text{data } \text{Tm } \alpha : \text{Set} \text{ where }
\phantom{\text{V}} & : (x : \text{Name } \alpha) \rightarrow \text{Tm } \alpha \\
\phantom{\text{\_ \_}} & : (t \ u : \text{Tm } \alpha) \rightarrow \text{Tm } \alpha \\
\phantom{\text{x}} & : \forall \ \{\beta\} \ (\ell : \alpha \leftrightarrow \beta) \ (t : \text{Tm } \beta) \rightarrow \text{Tm } \alpha \\
\text{Let} & : \forall \ \{\beta\} \ (\ell : \alpha \leftrightarrow \beta) \ (t : \text{Tm } \alpha) \ (u : \text{Tm } \beta) \rightarrow \text{Tm } \alpha
\end{align*}$$

Using only the function \texttt{strengthen?} one can build our usual functions \texttt{fv} and \texttt{rm} to compute the list of free variables and remove a name from a list of names:
6.3. LINKS: BINDERS AS WORLD RELATIONS

6.3.2 Implementations

An appealing definition for nominal links would to pair a binder \( b \) and a proof that \( \beta \) is equal to \( b \triangleleft \alpha \) this is called a weak link in \[\text{Pouillard and Pottier, 2010}\]. However to support the weakening operation a fresh-for proof is required. Hence a nominal link is made of a binder \( b \), a proof that \( b \# \alpha \), and a proof that \( \beta \) is equal to \( b \triangleleft \alpha \), this is called a strong link in \[\text{Pouillard and Pottier, 2010}\]. Our implementation reuses the type \textit{Supply} which already packages a binder plus a fresh-for proof. Our nominal implementation
is straightforward. The weakening operation uses a coercion. The strengthening operation boils down to our function \texttt{export}\textsuperscript{\texttt{N}}\texttt{?}. The operation \texttt{nameOf} returns the underlying binder converted to a name. In \texttt{Agda} we have the following module:

\begin{verbatim}
module Nom where
  record _→_ α β : Set where
    constructor _→_
    field
      supply : Supply α
    open Supply supply
    field
      β-def : β ≡ seed\textsuperscript{B} ⊆ α

  weaken : ∀ {α β} → α ⊣→ β → Name α → Name β
  weaken (supply , ≡.refl) = coerce\textsuperscript{N} (Supply.seed⊆ supply)

  strengthen? : ∀ {α β} → α ⊣→ β → Name β →? Name α
  strengthen? (_ , ≡.refl) = export\textsuperscript{N}?

  nameOf : ∀ {α β} → α ⊣→ β → Name β
  nameOf ((seed\textsuperscript{B} , _) , ≡.refl) = name\textsuperscript{B} seed\textsuperscript{B}

  nomLinks : Link _→_
  nomLinks = mk weaken strengthen? nameOf

\end{verbatim}

We now do the same with de Bruijn indices. A link in de Bruijn style is just a proof that the inner world $\beta$ is equal to the outer world $\alpha$ shifted by one. The weakening is the successor function and the strengthening the predecessor function. The function \texttt{nameOf} returns 0:
6.3. LINKS: BINDERS AS WORLD RELATIONS

module DeBruijn where

↪

→

:_→_: (α β : World) → Set

α ↪ β = β ≡ (α ↑1)

weaken : ∀ {α β} → α ↪ β → Name α → Name β
weaken ≡ .refl = suc↑

strengthen? : ∀ {α β} → α ↪ β → Name β →? Name α
strengthen? ≡ .refl = pred↑

nameOf : ∀ {α β} → α ↪ β → Name β
nameOf ≡ .refl = zero↑

deBruijnLinks : Link _→_
deBruijnLinks = mk weaken strengthen? nameOf

6.3.3 Building links and terms

In order to build terms we need to introduce more operations, though. Indeed we have no initial links to use. To this end we introduce a simple interface to build links. This interface provides two operations: init and next. More precisely these operations work on links where the inner world is made existential. Here is our interface in Agda:

record FreshLink {_→_} {link : Link _→_} : Set where
  constructor mk
  open Link link

Fresh : World → Set
Fresh α = ∃[ β ](α ↪ β)

field
  -- An infinite ‘‘chain’’ of binding-links
  init : Fresh ⊥
  next : ∀ {α}(x : Fresh α) → Fresh (proj₁ x)

As we see in the type of the operation next, the links are chained. Let fresh be a value of type Fresh α. The outer world of next fresh is the inner world of fresh. Here is our straightforward nominal implementation of the FreshLink interface based on operations on name supplies:
module NomFresh where

init : Fresh ∅
init = _, 0 ⊥, ≡.refl

next : ∀ {α} (x : Fresh α) → Fresh (proj₁ x)
next (_, s, ≡.refl) = _, suc s, ≡.refl

nomFreshLinks : FreshLink nomLinks
nomFreshLinks = mk init next

The de Bruijn implementation is so trivial that Agda infers most of the
definition by unification:

module DeBruijnFresh where

init : Fresh ∅
init = _, ≡.refl

next : ∀ {α} (x : Fresh α) → Fresh (proj₁ x)
next _ = _, ≡.refl

deBruijnFreshLinks : FreshLink deBruijnLinks
deBruijnFreshLinks = mk init next

Building terms is a matter of allocating binding-links and weakening
names such that they are in the expected world. To illustrate the construc-
tion of terms here are two examples:

idTm : Tm ∅
idTm = x x x \!
where x = proj₂ init
   xᵀm = V (name₀f x)

apTm : Tm ∅
apTm = x x (x y (xᵀm • yᵀm))
where x = proj₂ init
   y = proj₂ (next init)
   xᵀm = V (weaken y (name₀f x))
   yᵀm = V (name₀f y)

6.3.4 Kits and traversals

We now leverage our technique to build kits and traversals. Adapting the
work that we did in the nominal style is mostly straightforward. Kits are
made of a function to operate on names and a function to operate on links. To operate on a link the function \( \text{commEnv} \), given a link and an environment, returns both a new link and a new environment. The type \( \text{Comm} \) is the most difficult part of these traversals and is already described in our 2010 work [Pouillard and Pottier, 2010]:

\[
\text{Comm} : (_\leadsto_ : (\alpha \beta : \text{World}) \to \text{Set}) \to \text{Set}
\]

\[
\text{Comm} _\leadsto_ = \forall \{\alpha \beta \gamma\} \to (\alpha \leftrightarrow \beta \times \alpha \leadsto \gamma)
\to \exists [\delta](\gamma \leftrightarrow \delta \times \beta \leadsto \delta)
\]

A traversal kit is then made of a function \( \text{trName} \) and a function \( \text{commEnv} \). As before the kit is parameterized over the type of environments \( \text{Env} \) and the type of results \( \text{Res} \).

\[
\text{record} \; \text{TrKit} \; (\text{Env} : (\alpha \beta : \text{World}) \to \text{Set})
\;
\;
\text{constructor} \; \text{mk}
\text{field}
\text{trName} : \forall \{\alpha \beta\} \to \text{Env} \alpha \beta \to \text{Name} \alpha \to \text{Res} \beta
\;
\text{commEnv} : \text{Comm} \; \text{Env}
\]

We now build the renaming kit. Again the solution is close to the nominal one even if it works for de Bruijn style links as well. Here the supply is of type \( \text{Fresh} \). The function \( \text{importFun} \) takes two links and lifts a function over names in outer worlds \( \alpha \) and \( \beta \) to a function over names in inner worlds \( \gamma \) and \( \delta \). The function \( \text{importFun} \) then form the core part of the commutation function for renaming environments. As with nominal kits the environment is a mapping of names from the input world to the output world. This mapping freshens the bound variables and uses a name supply to do so.

\[
\text{importFun} : \forall \{\alpha \beta \gamma \delta\} \to \alpha \leftrightarrow \gamma
\to \beta \leftrightarrow \delta
\to (\text{Name} \alpha \to \text{Name} \beta)
\to (\text{Name} \gamma \to \text{Name} \delta)
\]

\[
\text{importFun} \; \ell_1 \; \ell_2 \; f \; x
\text{with} \; \text{strengthen?} \; \ell_1 \; x
\text{... | nothing = nameOf} \; \ell_2
\text{... | just} \; x' = \text{weaken} \; \ell_2 \; (f \; x')
\]

\[
\text{RenameEnv} : (\alpha \beta : \text{World}) \to \text{Set}
\]
CHAPTER 6. VARIATIONS AND RELATED WORK

\[ \text{RenameEnv } \alpha \beta = \text{Fresh } \beta \times (\text{Name } \alpha \rightarrow \text{Name } \beta) \]

\[ \text{renameKit : TrKit RenameEnv Name} \]
\[ \text{renameKit } = \text{mk proj}_2 \text{comm} \]
\[ \text{where} \]
\[ \text{comm : Comm RenameEnv} \]
\[ \text{comm } (x , (_, y) , f) \]
\[ = (_, y , \text{next } (_, y) , \text{importFun } x y f) \]

We now define the traversal function for our particular type for terms. As usual the environment is carried down the recursive function. The function \( \text{trName} \) is called at variables. The function \( \text{commEnv} \) is used at name-abstractions. Given the link found in the name-abstraction and the current environment, the function \( \text{commEnv} \) returns both a new link to close the resulting name-abstraction and a new environment to continue the traversal on subterms in scope of the name-abstraction:

\[ \text{module Tr } \{ \text{Env } : (\alpha \beta : \text{World}) \rightarrow \text{Set} \} \]
\[ \text{where} \]
\[ \text{open TrKit trKit} \]
\[ \text{tr } : \forall \{ \alpha \beta \} \rightarrow \text{Env } \alpha \beta \rightarrow \text{Tm } \alpha \rightarrow \text{Tm } \beta \]
\[ \text{tr } \Gamma (V x) = \text{trName } \Gamma x \]
\[ \text{tr } \Gamma (t \cdot u) = \text{tr } \Gamma' t \cdot \text{tr } \Gamma' u \]
\[ \text{tr } \Gamma (\lambda \ell t) \text{ with } \text{commEnv } (\ell , \Gamma) \]
\[ \ldots \]
\[ \text{tr } \Gamma (\text{Let } \ell t u) \text{ with } \text{commEnv } (\ell , \Gamma) \]
\[ \ldots \]
\[ \text{We put our traversal function at work by using the renaming kit to build a renaming function. Since our renaming kit is producing names and our traversal function expecting a kit which produces terms we have to lift it. The function } \text{kitVar} \text{ is a kit transformer applying the constructor } V \text{ to the result of the input function } \text{trName}. \text{ Then the function } \text{renameTm} \text{ gives the kit and the initial arguments to the traversal function.} \]

\[ \text{kitVar } : \forall \{ \text{Env} \} \rightarrow \text{TrKit Env Name } \rightarrow \text{TrKit Env Tm} \]
\[ \text{kitVar } (\text{mk } \text{trName } \text{commEnv}) = \text{mk } (\lambda \Gamma \rightarrow V \circ \text{trName } \Gamma) \text{ commEnv} \]

\[ \text{renameTm } : \forall \{ \alpha \beta \} \rightarrow \text{Fresh } \beta \rightarrow (\text{Name } \alpha \rightarrow \text{Name } \beta) \rightarrow \text{Tm } \alpha \rightarrow \text{Tm } \beta \]
\[ \text{renameTm } (f r) = \text{Tr.tr } (\text{kitVar } \text{renameKit}) (f r) \]
With the function `renameTm` we can lift the function `weaken` from names to terms. In this function the input link serves both as the initial weakening function for free names and as a name supply for the freshening purposes. Here is the function `weakenTm`:

\[
\text{weakenTm} : \forall \{\alpha \beta\} \to \alpha \leftrightarrow \beta \to \text{Tm} \alpha \to \text{Tm} \beta
\]

\[
\text{weakenTm} \ell \ t = \text{renameTm} (\text{next } (\_ , \ell)) (\text{weaken } \ell) \ t
\]

Our last application is a capture avoiding substitution function. To simplify matters we build a substitution kit specialized for our term type. The only important difference with the renaming kit is the use of the function `weakenTm` instead of `weaken`. The kit is then given to our traversal function to produce the function `substTm`. We then specialize our substitution function to replace a name/link by a closed term in a term with just this free variable. Finally we write the function \(\beta\text{-red}\) which reduces the \(\beta\)-redex on the root of the term if there is one.

\[
\text{SubstEnv} : (\alpha \beta : \text{World}) \to \text{Set}
\]

\[
\text{SubstEnv} \alpha \beta = \text{Fresh} \beta \times (\text{Name} \alpha \to \text{Tm} \beta)
\]

\[
\text{substKit} : \text{TrKit SubstEnv Tm}
\]

\[
\text{substKit} = \text{mk proj}_2 \text{ comm}
\]

\[
\text{where}
\]

\[
\text{importFunTm} : \forall \{\alpha \beta \gamma \delta\} \to \alpha \leftrightarrow \gamma
\]

\[
\to \beta \leftrightarrow \delta
\]

\[
\to (\text{Name} \alpha \to \text{Tm} \beta)
\]

\[
\to (\text{Name} \gamma \to \text{Tm} \delta)
\]

\[
\text{importFunTm} \ell_1 \ell_2 f x
\]

\[
\text{with strengthen? } \ell_1 x
\]

\[
\ldots \mid \text{nothing} = \text{V } (\text{nameOf } \ell_2)
\]

\[
\ldots \mid \text{just } x' = \text{renameTm} (\text{next } (\_ , \ell_2)) (\text{weaken } \ell_2) (f \ x')
\]

\[
\text{comm} : \text{Comm SubstEnv}
\]

\[
\text{comm} (x , (\_ , y) , f)
\]

\[
= (\_ , y , (\text{next } (\_ , y) , \text{importFunTm} \ x \ y \ f))
\]

\[
\text{substTm} : \forall \{\alpha \beta\} \to \text{Fresh} \beta \to (\text{Name} \alpha \to \text{Tm} \beta) \to \text{Tm} \alpha \to \text{Tm} \beta
\]

\[
\text{substTm} \ fr \ f = \text{Tr.tr substKit } (fr , f)
\]

\[
\_[\_ := \_] : \forall \{\alpha\} \to \text{Tm} \alpha \to \emptyset \leftrightarrow \alpha \to \text{Tm} \emptyset \to \text{Tm} \emptyset
\]
CHAPTER 6. VARIATIONS AND RELATED WORK

Conclusion  By instantiating links to be either nominal links or de Bruijn links we obtain the corresponding implementation of the $\beta$-reduction of $\lambda$-terms. In contrast to our previous work [Pouillard and Pottier, 2010] we simplified the presentation to only retain one kind of binding-link. To reuse the terminology of [Pouillard and Pottier, 2010] we keep only the strong links. We think the purpose of this binding-link abstraction is to be more focused on a clean and simple interface than a comprehensive and precise interface. Indeed precision has been achieved in our library through binders, world operations, world inclusions, and operations on names. The binding-link abstraction hides details about the representation. While a nominal binder can shadow the previous one, a link, thanks to the fresh-for proof, cannot. While a de Bruijn binder is canonical, a link is not. While we can perform arithmetic with de Bruijn indices in our library, with links we cannot. Yet terms with binding-links can be equipped with kits and traversals. In short the paradigm is still very expressive but less flexible.

6.4 Combining nominal and nameless styles

The support for de Bruijn indices and de Bruijn levels, has been introduced by only adding new items to the interface. Neither the interface, the implementation nor the logical relation need to be altered, only extended.

Here we present one of the multiple combinations that could be made. We have two constructors for $\lambda$-abstraction, one in nominal style and one in de Bruijn indices style. Right after, we show the function $fv$ which produces no surprises.

```haskell
data Tm α : Set where
  V  : (x : Name α) → Tm α
  λN : ∀ b (t : Tm (b α)) → Tm α
  λB : (t : Tm (α ↑1)) → Tm α
  _·_ : (t u : Tm α) → Tm α
```
6.4. COMBINING NOMINAL AND NAMELESS STYLES

$$fv : \forall \{\alpha\} \rightarrow Tm\ \alpha \rightarrow List\ (Name\ \alpha)$$

$$fv(V\ x) = [\ x\ ]$$

$$fv(fct \cdot\ arg) = fv\ fct \oplus\ fv\ arg$$

$$fv(x^{B} b\ t) = rm\ b\ (fv\ t)$$

$$fv(x^{D} t) = rm_{0}\ (fv\ t)$$

We now show two variants of a term which combines those two styles of bindings. One thing to notice is that even if a name is introduced in a nominal style, one has to shift it to cross de Bruijn style binder. The first variant binds the first name in nominal style and the second name in the de Bruijn style. To reach the nominal binder from the inside $suc^{N}$ is used.

The second variant binds the first name in de Bruijn style and the second in nominal style. To cross the nominal binder, the de Bruijn occurrence needs to be coerced showing that two worlds are included:

$$apTm_{1} : \forall \{\alpha\} \rightarrow Tm\ \alpha$$

$$apTm_{1} = x^{B} x (x^{D} (V\ (suc^{N} (name^{B} x)) \cdot\ V\ (0\ N)))$$

where $x = 42^{B}$

$$apTm_{2} : Tm\ \emptyset$$

$$apTm_{2} = x^{D} (x^{N} x (V\ (coerce^{N} pf\ (0\ N)) \cdot\ V\ (name^{B} x)))$$

where $x = 42^{B}$

$$pf = \{!\ \text{proof omitted}!\}$$

An attractive feature of this combined style would be to partially convert to de Bruijn indices. Once converted, the canonical structure can be used. Since the conversion to de Bruijn indices requires to maintain a mapping from nominal names to de Bruijn indices we build a more general renaming function. Our renaming function (called $ren$) is similar to $renameTm^{D}$ (section 5.3.4) but accepts nominal bindings as well. It is similar to $renameTm$ (section 3.2) but does not require a name supply argument to build the result term. This function $ren$ hence both converts to de Bruijn indices and applies the supplied function on free variables. To build the function $ren$, the user-supplied function on names must be adapted to cross name-abstractions. We reuse the function $protect^{\uparrow 1}$ from section 5.3.4 which is adapted when both the source and target abstractions are de Bruijn indices. We build a variant of the function $protect^{\uparrow 1}$ called $protect^{\downarrow 1}$ which works when the source abstraction is nominal and the target abstraction is de Bruijn.
Using this renaming function we build a simple normalization function which just supplies the identity function as the renaming:

\[
\text{norm} : \forall \{\alpha\} \rightarrow \text{Tm} \alpha \rightarrow \text{Tm} \alpha
\]
\[
\text{norm} = \text{ren id}
\]

Using this combined approach one may loose the convenience of nominal bindings. To recover this convenience, we build a function called \(\text{openTm}\) such as in section 6.1. The function \(\text{openTm}\) takes a name supply \(s\) and an open de Bruijn term \(t\). The function renames the de Bruijn index zero to the first name of the name supply. We then define a simple function called \(\text{nomview}\) which converts the toplevel \(\lambda\)-abstraction from de Bruijn to nominal. This function \(\text{nomview}\) enables to look at the terms as though there were only nominal \(\lambda\)-abstractions. However using \(\text{nomview}\) and \(\text{openTm}\) incurs the limitations we discussed in section 6.1, namely convenience, performance, and non-structural recursion.

\[
\text{openTm} : \forall \{\alpha\} \ (s : \text{Supply} \alpha) \rightarrow \text{Tm} \ (\alpha \uparrow 1) \rightarrow \text{Tm} \ (\text{seed}^B \ s \downarrow \alpha)
\]
\[
\text{openTm} \ {\{\alpha\}} \ (b \ , \ b\#) = \text{ren f where}
\]
\[
f : \text{Name} \ (\alpha \uparrow 1) \rightarrow \text{Name} \ (b \downarrow \alpha)
\]
\[
f = \text{exportWith} \ (\text{name}^B \ _) \ (\text{coerce}^B \ (\subseteq \# \ b\#) \circ \text{pred}^N)
\]

\[
\text{nomview} : \forall \{\alpha\} \rightarrow \text{Supply} \alpha \rightarrow \text{Tm} \alpha \rightarrow \text{Tm} \alpha
\]
\[
\text{nomview} \ s \ (\chi^D \ t) = \chi^N \ _ \ (\text{openTm} \ s \ t)
\]

A tantalizing change would be to include new constructors to represent the open and close operations internally. This would enable a lazy opening and closing for terms. For instance we could try to add these data constructors:
6.5. NOMINAL TYPES

Close : ∀ {α} b → Tm (b ◼ α) → Tm (α ↑1)
Open : ∀ {α b} → b # α → Tm (α ↑1) → Tm (b ◼ α)

However, we did not go very far with these constructors. Pattern-matching on these is already limited given the indices of the result type are not invertible. Using explicit type equalities helps to go a bit further but not much:

Close : ∀ {α β} (eq : β ≡ α ↑1) b → Tm (b ◼ α) → Tm β
Open : ∀ {α β b} (eq : β ≡ b ◼ α) → b # α → Tm (α ↑1) → Tm β

We have explored one particular combination, namely combining nominal and de Bruijn indices styles. We have shown how to build terms, but also how to get a canonical form using de Bruijn indices. We have also shown how to convert one de Bruijn binding to a nominal one. Exploring other combinations is left as a topic for further research. This may include combinations with de Bruijn levels, higher-order representations (such as our normalization by evaluation function in section 3.4), nominal binders with fresh-for proofs to maintain distinct binders, etc.

6.5 Nominal types

In this section we successively describe various specification languages to describe languages. More concretely a specification language enables to write type definitions and their binding structure. In section 6.5.1, we describe nominal signatures as used in FRESHML-LITE [Shinwell et al., 2003]. We first describe signatures with a single sort of atoms and then generalize to multiple sorts. We then focus on languages with pattern types such as FRESHML and FRESH OCAML in section 6.5.1, Caml in section 6.5.2 and BINDERS UNBOUND in section 6.5.3.

6.5.1 FreshML & Fresh OCaml types

FRESHML [Shinwell et al., 2003] is a programming language, designed by Mark R. Shinwell, Andrew M. Pitts and Murdoch J. Gabbay. The language is designed to make programming with binders simple. The language is an ML-like language augmented with types and language constructs to deal with names and binders. The language has a conventional call-by-value operational semantics and a type system preventing to break name abstraction. This means that two α-equivalent terms cannot be distinguished within the language. The language offers an adequate encoding of nominal terms (to be described shortly) and guarantees that the identity of a bound name cannot be observed. However, it does not prevent a newly generated atom from escaping its scope.
Fresh OCAML [Shinwell and Pitts, 2005] is an extension of the OCAML [Leroy et al., 2005] language. This language extension enriches OCAML with a primitive type for names and one type construction for name abstractions. From a language design point of view, Fresh OCAML brings the features of FreshML to OCAML.

FreshML-Lite is a light version of FreshML without pattern types and restricted to a single sort of atoms. Indeed FreshML and Fresh OCAML have a simple notion of pattern types that we do not treat here. Pattern types are covered in section 6.5.2 and 6.5.3 about Cαml and Binders Unbound. About multiple sorts we show how to handle those and then go back to a single sort to simplify matters.

Nominal terms are the values described by nominal signatures. Here is the definition of a nominal signature as of Definition 2.1 of “Nominal Unification” [Urban et al., 2004]:

“A nominal signature is specified by: a set of sorts of atoms (typical symbol $\nu$); a disjoint set of sorts of data (typical symbol $\delta$); and a set of function symbols (typical symbol $f$), each of which has an arity of the form $\tau \rightarrow \delta$. Here $\tau$ ranges over (compound) sorts given by the grammar $\tau ::= \nu | \delta | 1 | \tau \times \tau | <\nu>\tau$. Sorts of the form $<\nu>\tau$ classify terms that are binding abstractions of atoms of sort $\nu$ over terms of sort $\tau$. We will explain the syntax and properties of such terms in a moment.”

Our goal now is to show how we can describe any nominal signature using our library. We could expect sorts of atoms, sorts of data and compound sorts to be translated directly as types in Agda, and thus to have type Set (no index). However this would be incompatible with our technique which indices names (atoms) and terms by worlds. We call expression types what corresponds to the compound sorts in nominal signatures. The term expression takes all its sense when combined with pattern types that we will see later. In Agda we call the type of expression types $E$.

Nominal signatures on one atom sort We now describe the interface to build and combine expression types and nominal signatures. For simplicity we assume that only one sort of atom is used, that we call $\nu$. The first component is called $\nu^*$ and corresponds to atoms of sort $\nu$. The second component is called $1^*$ and corresponds to the unit expression type. We can take the product of two expression types with $\times^*$. Finally the expression type $<\nu>^* \tau$ classifies the terms that are name-abstractions of atoms of sort $\nu$ over terms of type expression $\tau$. Note that since we constrained the interface to a single sort of atoms, name-abstraction expects only one argument, the expression type. To declare a function symbol we introduce $\mapsto^*$ which takes two expression types and returns an Agda type (i.e. Set). In Agda we have the following declarations for the interface:
We now give an example of the use of this interface to build a nominal signature. We use Agda’s data type definitions to handle the introduction of data sorts, function symbols, and the handling of recursion. This example describes a fragment of ML. We recall as a comment how this nominal signature was originally written [Urban et al., 2004].

{- A Nominal Signature:
Example 2.2 from ‘Nominal Unification’

sort of atoms: vid
sort of data: exp
function symbols:
vr : vid → exp
app : exp × exp → exp
lam : <vid>exp → exp
lv : exp × <vid>exp → exp
lf : <vid>((<vid>exp) × exp) → exp
-}

As we can see, the definition of a nominal signature can be easily done within our system. The resulting Exp type is fully usable. As an example we give the definition of the function fv.
\[
\begin{align*}
fv : \text{Exp} & \rightarrow^\alpha \text{List}^\alpha \nu^\alpha \\
fv (\text{vr} \ x) & = [x] \\
fv (\text{app} (t, u)) & = fv \ t ++ fv \ u \\
fv (\text{lam} (b, t)) & = \text{rm} \ b \ (fv \ t) \\
fv (\text{lv} (t, b, u)) & = fv \ t ++ \text{rm} \ b \ (fv \ u) \\
fv (\text{lf} (\text{bf}, (b, t), u)) & = \text{rm} \ \text{bf} \ (\text{rm} \ b \ (fv \ t) ++ fv \ u)
\end{align*}
\]

This function \(fv\) already reveals parts of the definitions for our nominal signature combinators that we now present in detail. We have not much other options than using \(\text{Name}\) as the definition for \(\nu^\alpha\). This forces \(E\) to be \(\text{World} \rightarrow \text{Set}\). This last definition can also be read as “expression types are the world-indexed types” which should come as no surprise as it captures the very intuition behind our system. The unit type expression \((1^\alpha)\) ignores the world index and yields Agda’s unit type. The product of expression types \((\times^\alpha)\) distributes the world to the subcomponents. Name abstraction pairs a binder and a sub-expression type whose world is properly extended. Finally, the combinator to declare a function symbol \(\rightarrow^\alpha\) distributes to the underlying arrow type but also quantifies over the world. Here are the definitions in Agda.

```agda
module MonoSortedNominalSignature where
  E : Set₁
  E = World → Set

  \(\nu^\alpha\) : E
  \(\nu^\alpha\) = Name

  \(1^\alpha\) : E
  \(1^\alpha\) = ⊤ -- ⊤ is Agda’s unit type

  \(\times^\alpha\) : E → E → E
  \((E₁ \times^\alpha E₂) \alpha = E₁ \alpha \times E₂ \alpha\)

  \(<\nu>^\alpha\) : E → E
  \((<\nu>^\alpha E) \alpha = \exists b \{ E (b \triangleleft \alpha)\}\)

  \(\rightarrow^\alpha\) : E → E → Set
  \(E₁ \rightarrow^\alpha E₂ = \forall \{ \alpha \} → E₁ \alpha → E₂ \alpha\)
```

One might want to unfold the type of a few symbols we defined. Modulo currying, the symbols \(\text{Exp, vr, lam and fv}\) correspond to \(\text{Tm, V, x and fv}\) from section 2.2:
Multi-sorted nominal signatures  We now enrich our expression types with multiple sorts of atoms. We call \texttt{Sort} the type of atom sorts. This type \texttt{Sort} is actually part of the definition of a nominal signature and thus is not part of the interface. Actually, the interface is parameterized over the type for atom sorts. We rename the $\nu^e$ as \texttt{Name$^e$} in this version. \texttt{Name$^e$} associates an $\mathcal{E}$ to each value of \texttt{Sort}. The unit, list and product for expression types are now derived from the more general combinators \texttt{Neutral$^e$}, \texttt{Neutral1$^e$}, \texttt{Neutral2$^e$}, etc. These combinators respectively lift any type $\texttt{Set}$, $\texttt{Set} \to \texttt{Set}$, $\texttt{Set} \to \texttt{Set} \to \texttt{Set}$ to $\mathcal{E}$, $\mathcal{E} \to \mathcal{E}$, $\mathcal{E} \to \mathcal{E} \to \mathcal{E}$, etc. The expression type $\langle \nu^e \rangle \tau$ classifies the terms that are name-abstractions of atoms of sort $\nu$ over terms of type expression $\tau$.

We keep the other combinators unchanged. In \texttt{Agda} we have the following declarations for the interface:

\begin{verbatim}
module MultiSortedNominalSignature
  (Sort : Set) (_==_ : (x y : Sort) → Bool) where

  E     : Sort → Set
  Name$^e$ : Sort → E
  $\langle \_ \rangle^e$ : Sort → E → E
  $\_\_^e$ : E → E → Set
  Neutral$^e$ : Set → E
  Neutral1$^e$ : (Set → Set) → (E → E)
  Neutral2$^e$ : (Set → Set → Set) → (E → E → E)

  1$^e$ : E
  1$^e$ = Neutral$^e$ ⊤

  List$^e$ : E → E
  List$^e$ = Neutral1$^e$ List

  _×$^e_ : E → E → E
  _×$^e_ = Neutral2$^e$ _×_  

\end{verbatim}

To illustrate this new interface and the use of multiple sorts we present a simple signature for System $F$ where type variables are distinguished from term variables. Notice that apart from the boring definition for \_==\_ our
embedded language for signatures is lightweight.

```haskell
module NominalSignatureExample where

data Sort : Set where
  vtm vty : Sort

  _==_ : (x y : Sort) → Bool
  vtm == vtm = true
  vty == vty = true
  vtm == vty = false
  vty == vtm = false

open MultiSortedNominalSignature nomPa Sort _==_

data Ty : E where
  var : Name vty ↦ⁿ Ty
  arr : Ty ×ⁿ Ty ↦ⁿ Ty
  all : < vty >ⁿ Ty ↦ⁿ Ty

data Tm : E where
  vr : Name vtm ↦ⁿ Tm
  app : Tm ×ⁿ Tm ↦ⁿ Tm
  lam : Ty ×ⁿ < vtm >ⁿ Tm ↦ⁿ Tm
  App : Tm ×ⁿ Ty ↦ⁿ Tm
  Lam : < vty >ⁿ Tm ↦ⁿ Tm

We show that computing the free type variables in both types and terms
can be programmed without any extra difficulty. Here the type system not
only prevents from leaking bound names but also prevents from mixing the
two sorts of variables.

fvtyTy : Ty ↦ⁿ List⁻¹ (Name⁻¹ vty)
fvtyTy (var x) = [ x ]
fvtyTy (arr (σ , τ)) = fvtyTy σ ++ fvtyTy τ
fvtyTy (all (b , τ)) = rm b (fvtyTy τ)```

156  

CHAPTER 6. VARIATIONS AND RELATED WORK
6.5. NOMINAL TYPES

```
fvtyTm : Tm →¹ List¹ (Name¹ vty)
fvtyTm (vr x) = []
   -- [ x ] would not type-check
fvtyTm (app (t , u)) = fvtyTm t ++ fvtyTm u
fvtyTm (lam (τ , b , t)) = fvtyTy τ ++ fvtyTm t
   -- rm b ... would not type-check
fvtyTm (App (t , τ)) = fvtyTm t ++ fvtyTy τ
fvtyTm (Lam (b , t)) = rm b (fvtyTm t)
```

We can now turn to the implementation of the multi-sorted interface. Expression types are no longer indexed by a single world but by a collection of worlds. This collection of worlds is itself indexed by atom sorts, and represented by a function from sorts to worlds. The combinator `Name¹` is the type `Name` in the world given by looking up the world associated to the sort `ν`. The combinator `<_>_¹` needs to update the collection of worlds at the given atom sort. To do so we define the function `_[]=_` to do this update. The combinators `Neutral¹`, `Neutral1¹`, and `Neutral2¹` are distributing the index to the subcomponents. Since `λ A → Ix → A` is an applicative functor (often called Reader) for all index types `Ix`, the neutral combinators correspond to `pure`, `liftA`, and `liftA2` of this applicative functor. Here is the Agda implementation.

```agda
module MultiSortedNominalSignature
  (Sort : Set) (_==_ : (x y : Sort) → Bool) where

  E : Set₁
  E = (Sort → World) → Set

  Name¹ : Sort → E
  Name¹ ν Γ = Name (Γ ν)

  _[_:=_] : (Sort → World) → Sort → World → (Sort → World)
  (Γ [ ν := α ]) ν′ = if ν == ν′ then α else Γ ν′

  <_>_¹ : Sort → E → E
  (< ν >¹ E) Γ = ∃[ b ](E (Γ [ ν := b ∅ Γ ν ]))
```
\textbf{Neutral}^e : \text{Set} \rightarrow \mathcal{E}
\text{Neutral}^e \mathbb{A} = \mathbb{A}

\text{Neutral}^1^e : (\text{Set} \rightarrow \text{Set}) \rightarrow (\mathcal{E} \rightarrow \mathcal{E})
\text{Neutral}^1^e \mathbb{F} \mathbb{E} \mathbb{\Gamma} = \mathbb{F} (\mathbb{E} \mathbb{\Gamma})

\text{Neutral}^2^e : (\text{Set} \rightarrow \text{Set} \rightarrow \text{Set}) \rightarrow (\mathcal{E} \rightarrow \mathcal{E} \rightarrow \mathcal{E})
\text{Neutral}^2^e \text{Op} \mathbb{E}^1 \mathbb{E}^2 \mathbb{\Gamma} = \text{Op} (\mathbb{E}^1 \mathbb{\Gamma}) (\mathbb{E}^2 \mathbb{\Gamma})

\text{\texttt{1}}^e : \mathcal{E}
\text{\texttt{1}}^e = \text{Neutral}^e \top

\text{List}^e : \mathcal{E} \rightarrow \mathcal{E}
\text{List}^e = \text{Neutral}^1^e \text{List}

\text{\texttt{-}×\texttt{-}}^e : \mathcal{E} \rightarrow \mathcal{E} \rightarrow \mathcal{E}
\text{\texttt{-}×\texttt{-}}^e = \text{Neutral}^2^e \text{\texttt{-}×\texttt{-}}

\textbf{FreshML types} In addition to nominal signatures, \textsc{freshml} and \textsc{fresh ocaml} support function types in their signatures. This can be taken into account by adding an arrow combinator. We introduce it in two flavors:

\text{\texttt{-}→\texttt{-}}^e : \mathcal{E} \rightarrow \mathcal{E} \rightarrow \mathcal{E}
(E_1 \rightarrow^e \mathbb{E}_2) \alpha = E_1 \alpha \rightarrow E_2 \alpha

\text{\texttt{-}⇒\texttt{-}}^e : \mathcal{E} \rightarrow \mathcal{E} \rightarrow \mathcal{E}
(E_1 \Rightarrow^e \mathbb{E}_2) \alpha = \forall \{\beta\} \rightarrow \alpha \subseteq \beta \rightarrow (E_1 \rightarrow^e \mathbb{E}_2) \beta

\Rightarrow\text{-to-\rightarrow} : \forall \{E_1 \mathbb{E}_2\} \rightarrow (E_1 \Rightarrow^e \mathbb{E}_2) \Rightarrow^e (E_1 \rightarrow^e \mathbb{E}_2)
\Rightarrow\text{-to-\rightarrow} f = f \subseteq\text{-refl}

We introduced the latter when defining a normalization by evaluation algorithm in section 3.4. Moreover the latter version is generally more useful than the former since it can be “imported” by merging the given inclusion witness. Here is how to coerce such a function:

\text{Coe} : \mathcal{E} \rightarrow \text{Set}
\text{Coe} E = \forall \{\alpha \beta\} \rightarrow \alpha \subseteq \beta \rightarrow E \alpha \rightarrow E \beta

\text{coerce⇒\texttt{-}⇒}^e : \forall \{E_1 \mathbb{E}_2\} \rightarrow \text{Coe} (E_1 \Rightarrow^e \mathbb{E}_2)
\text{coerce⇒\texttt{-}⇒}^e \text{pf} f = f \circ \subseteq\text{-trans \texttt{pf}}
6.5.2 Coml types

Coml [Pottier, 2006] is both a tool and a language to describe data type with a binding structure. Coml has been developed by François Pottier. The tool takes data type definitions in a file and produces an OCAML [Leroy et al., 2005] module with OCAML data types and generated boiler plate code.

The data types language of Coml extends ML algebraic data types that we find in OCAML with annotations to describe the scoping rules. More precisely, Coml types extends nominal signatures with a notion of pattern types.

Coml data types are of two kinds: expression and pattern types. The expression kind is made to be used for, well, expression-like types. For instance our type \( \text{Tm} \) belongs to this kind, but type-expressions, statements, processes, etc. are expression types. We reuse the terminology of the previous section and call \( \mathcal{E} \) the type of expression types. As before we reuse the following primitive expression types: \( \text{Name}^e, \text{\_\_\_}^e, \text{Neutral}^e, \text{Neutral1}^e, \text{Neutral2}^e \). We reuse also the following derived expression types: \( \text{1}^e, \text{List}^e, \text{\_\_\_}^e \times^e \). In order for Coml to derive functions about these data types, functions are not allowed to appear in signatures. Name-abstractions are made of a pattern type and surrounded by \(<\_\_\_>\). Pattern types are called \( \mathcal{P} \) and also support various combinators to be described shortly.

\[
\begin{align*}
\text{-- A pattern type} \\
\mathcal{P} & : \text{Set}_1 \\
\text{-- Name abstraction} \\
<_\_\_> & : \mathcal{P} \to \mathcal{E}
\end{align*}
\]

Pattern types appear when we start a name-abstraction. Like expression types, pattern types are closed under products, and have the arrow \( \text{\_\_\_}^e \rightarrow \mathcal{P}^e \) to declare a data constructor (function symbol). In addition, patterns can be binders, or expression types with inner and outer annotations. Since pattern types embed expression types, base types can be lifted to patterns as well. Here are the signatures of the various forms of pattern types:
module Com1Types where

open MonoSortedNominalSignature public

Binder^ : \mathcal{P} \\
_p \times_p : \mathcal{P} \to \mathcal{P} \to \mathcal{P} \\
_p \rightarrow_p : \mathcal{P} \to \mathcal{P} \to \text{Set}

Outer^ : \mathcal{E} \to \mathcal{P} \\
Inner^ : \mathcal{E} \to \mathcal{P}

Neutral^ : \text{Set} \to \mathcal{P} \\
Neutral^ = Outer^ \circ \text{Neutral}^\circ \\
-- which is identical to \\
-- \text{Inner}^ \circ \text{Neutral}^\circ

-- List of patterns as special data type \\
-- since we could not reuse List here. \\
data List^\circ (\mathcal{P} : \mathcal{P}) : \mathcal{P} where \\
[ ] : 1^\circ \circ \text{List}^\circ \mathcal{P} \\
:: : \mathcal{P} \times^\circ \mathcal{P} \text{List}^\circ \mathcal{P} \circ \text{List}^\circ \mathcal{P}

To appear in pattern types, expression types are qualified as either outer or inner, and thus are respectively in-scope and out-of-scope of the surrounding abstraction. The disposition of binders and embedded expressions does not matter for Com1. The outer expressions are not affected by any binder of the pattern. Similarly all the inner expressions of a pattern are put in scope of all the binders introduced by the pattern.

Example To illustrate the use of expression and pattern types, we define our term type in the Com1 style and call it Exp. The lam case is made of a name-abstraction holding a pattern product with one binder and one inner term. The let case is more interesting and makes use of the Outer^\circ combinator to hold the first subterm out of the scope of the binder. As with nominal signatures we are using a data declaration to take care of introducing the constructors and dealing with the recursive nature of the type:

data Exp : \mathcal{E} where \\
\text{var} : \text{Name}^\circ \circ \text{Exp} \\
\text{app} : \mathcal{E} \circ \circ \mathcal{E} \circ \circ \mathcal{E} \\
\text{lam} : < \text{Binder}^\circ \circ \circ \text{Inner}^\circ \circ \mathcal{E} > \circ \circ \circ \mathcal{E} \\
\text{let}' : < \text{Binder}^\circ \circ \circ \text{Outer}^\circ \circ \circ \text{Inner}^\circ \circ \mathcal{E} > \circ \circ \circ \mathcal{E}
We continue our illustration of Comil’s expressiveness with local blocks of local definitions. To achieve this we simply reuse the declaration for let’ and wrap the binding with ListP:

\[
\text{let*} : \langle\text{List}^P (\text{Binder}^P \times^P \text{Outer}^P \text{Exp}) \times^P \text{Inner}^P \text{Exp} \rangle \rightarrow^P \text{Exp}
\]

To go from non-recursive blocks to recursive ones, a single step is required. Replacing OuterP by the InnerP annotation suffices to make all the bound names accessible to the right hand part of this construct.

\[
\text{rec} : \langle\text{List}^P (\text{Binder}^P \times^P \text{Inner}^P \text{Exp}) \times^P \text{Inner}^P \text{Exp} \rangle \rightarrow^P \text{Exp}
\]

We finally add some pattern-matching facilities to our small language. To do so, we introduce a pattern type named Pat. This type supports wildcard patterns, single binders, and pairs of patterns:

\[
data \text{Pat} : \prod^P \text{where}
\begin{align*}
\text{wildcard} & : \prod^P \rightarrow^P \text{Pat} \\
\text{binder} & : \text{Binder}^P \rightarrow^P \text{Pat} \\
\text{pair} & : \text{Pat} \times^P \text{Pat} \rightarrow^P \text{Pat}
\end{align*}
\]

Once we have patterns, we package them as branches. A branch holds a pattern, an optional guard, and a term associated with the pattern:

\[
\text{Branch} : \prod^E \\
\text{Branch} = \langle\text{Pat} \times^P \text{Inner}^P (\text{Maybe}^e \text{Exp}) \times^P \text{Inner}^P \text{Exp} \rangle
\]

The type Exp is then extended with a new match construct, which holds a scrutiny term and a list of branches:

\[
\text{match} : \text{Exp} \times^e \text{List}^e \text{Branch} \rightarrow^e \text{Exp}
\]

In our Agda development we show how to modularly define a free-variables function. To do so we define a combinator to compute the free variables for each form of expression types and pattern types. For pattern types we need no less than three actions to collect the inner free variables, the outer free variables, and to remove pattern binders from a list of free variables. Then at name-abstractions, free variables is the union of outer free variables and inner ones minus those bound by the pattern. In the end, one can build an \(\text{fv}\) function on terms whose body is made of combinators and exactly follow the definition of terms.
Behind the scenes  We now turn to the definitions needed to make these combinators work with our library. We focus on a single sort of atoms since we have shown how we can support multiple sorts. Expression types are not changed and directly reused from section 6.5.1.

The Comil change to expression types is the name-abstraction. However, before discussing the name-abstraction combinator, we need to cover pattern types. Pattern types are indexed by no less than two worlds, and an operator on worlds. Let $P$ be a pattern type, let $\alpha$ and $\beta$ be worlds, let $Op$ be an operator on worlds ($\text{World} \to \text{World}$), then $P \alpha \beta Op$ is a fully applied pattern type of type $\text{Set}$. The world $\alpha$ plays the role of the outer world, meaning before binders introduced by the pattern. The world $\beta$ is the inner world, meaning after all the binders introduced by the pattern. Thus, the worlds $\alpha$ and $\beta$ are outer and inner worlds with respect to the complete pattern found between name-abstraction brackets ($\langle...\rangle$). These two worlds $\alpha$ and $\beta$ are respectively used by $\text{Outer}^P$ and $\text{Inner}^P$ to pick the world of the expression type. Then the operator explains what the given pattern type changes to a world. If the pattern does not bind anything (as is the case of $\text{Outer}^P$ and $\text{Inner}^P$), then the operator is equal to the identity. Since a binder pattern binds one binder, the operator is equal to the corresponding binder insertion: $b \triangleleft \ldots$. Pattern products distribute $\alpha$ and $\beta$ to subcomponents. Subcomponents world operation get composed into a single operation to index the product. Finally the abstraction brackets package an operation and a fully applied pattern type whose outer world is the current world, the inner world is computed by applying $Op$ to the current world. Here are the definitions in Agda:

\[
\begin{align*}
P &: \text{Set}_1 \\
P &= (\alpha \beta : \text{World}) \ (Op : \text{World} \to \text{World}) \to \text{Set} \\

\text{Binder}^P &: P \\
\text{Binder}^P \alpha \beta Op &= \exists \ [ b ] (Op \equiv \triangleleft b) \\

\text{Outer}^P &: E \to P \\
\text{Outer}^P E \alpha \beta Op &= E \alpha \times Op \equiv \text{id} \\

\text{Inner}^P &: E \to P \\
\text{Inner}^P E \beta \beta Op &= E \beta \times Op \equiv \text{id} \\

data \times^P_\alpha (P_1 P_2 : P) : P \ where \\
\alpha : \forall \{Op_1 Op_2 \alpha \beta\} \\
\quad \to P_1 \alpha \beta Op_1 \\
\quad \to P_2 \alpha \beta Op_2 \\
\quad \to (P_1 \times^P P_2) \alpha \beta (Op_2 \circ Op_1)
\end{align*}
\]
6.5. NOMINAL TYPES

\[ \langle _, > : P \rightarrow E \]
\[ \langle P \rangle \alpha = \exists \text{[ Op ]}(P \alpha (\text{Op }\alpha) \text{Op}) \]

\[ \_\rightarrow \text{P} : \text{IP} \rightarrow \text{P} \rightarrow \text{Set} \]
\[ \_\rightarrow \text{P} : P_1 P_2 = \forall \{\alpha \beta \text{Op}\} \rightarrow P_1 \alpha \beta \text{Op} \rightarrow P_2 \alpha \beta \text{Op} \]

In the end, the world operation index of a pattern type could be replaced by a list of binders. However this abstract presentation enables more flexible uses. For instance here is the de Bruijn version of the combinator Binder:\(p:\)

\[
\text{Binder}^\text{bp} : \text{IP} \rightarrow \text{IP} \rightarrow \text{Set} \quad \text{Binder}^\text{bp} = \text{Op} \equiv \_\uparrow 1
\]

This de Bruijn combinator is useful in two ways. First one can imagine mixing Binder\(p:\) and Binder\(bp:\) as we have done in section 6.4. A second option would be to easily change the implementation from nominal to de Bruijn by just updating a single definition. This also shows that both nominal and de Bruijn are expressive enough to cover Coml data types.

A remark on linearity We can remark a subtle difference between Coml’s semantics for pattern types and the semantics provided by our definitions. In Coml if two binders in a same pattern are equal there is no shadowing. Such a pattern could be for instance: \(\lambda (x , x) \rightarrow \ldots\). In our setting there is shadowing and thus the order of binders in a pattern is relevant. This order is well-defined and specified on the combinator for products. In a pattern product, all the binders on the left comes before all the binders on the right. Thus those on the right can shadow those on the left. We actually recommend to deal with linearity before going to a well-scoped representation. If non-linear patterns have to be accepted, we recommend to turn the subsequent occurrences into free names and thus keep a linear pattern.

Conclusion In this section we explained how our embedded language to describe nominal signatures can scale to Coml signatures. This shows that all types that can be defined in Coml can also be defined in our system. However Coml also provides generated code to perform usual operations on data structures with names and binders. We do not address this part here but several generic programming techniques could be applied in our situation as well.

6.5.3 Connection with Binders Unbound

Stephanie Weirich, Brent Yorgey, and Tim Sheard develop a library called Binders Unbound [Weirich et al., 2011]. This library is written in Haskell and provides type level combinators to express data structures with binders.
Then through a mechanism of “data generic programming”, usual functions are generically provided for any combination of types. The main feature of Binders Unbound is to get all of these operations for free right after the type definition. It enables rapid prototyping where we directly focus on the code that matters to our program. The safety features are similar to those in FreshML, Fresh OCaml, and Caml. Name abstraction cannot be violated but names can escape their scope. However by providing many generic operations the number of bugs the programmer can introduce is reduced. Of course nothing prevents from combining both generic programming and a safer approach were names do not escape their scope. To achieve their goal of generic programming, an embedded language of combinators to define types is developed.

The language of combinators is modeled after expression and pattern types. Given our definitions of section 6.5.1 and section 6.5.2, we can adapt to the new combinators concisely. We focus on a single sort of atoms since we have shown how we can support multiple sorts. The first difference is the combinator $\text{Bind } P \ E$ which combines a pattern type $P$ and an expression type $E$. The binders in $P$ scope over the expression type $E$. This is equivalent to $< P \times^P \text{Inner}^P E >$ in Caml, but the combinator $<_,_>$ is not part of Binders Unbound. The combinator $\text{Embed}$ enables to embed an expression type into a pattern type. The combinator $\text{Embed}$ is equivalent to $\text{Outer}^P$ from Caml. The real new combinators are $\text{Rebind}$ and $\text{Rec}$. $\text{Rebind } P_1 P_2$ is a pattern type which binds both $P_1$ and $P_2$ like $P_1 \times^P P_2$ does. However, binders of $P_1$ also scope over the expressions embedded in $P_2$. $\text{Rec } P$ is a pattern types where binders of $P$ not only scope externally but scope over expressions embedded in $P$. As in Caml, functions cannot be used in data types.

We give definitions for $\text{Bind}$, $\text{Embed}$, $\text{Rebind}$ and $\text{Rec}$ using our definitions for Caml. The second world index ($\beta$) of pattern types is not used in Binders Unbound but would enable to combine them with Caml combinators.

$$\text{Bind} : P \rightarrow E \rightarrow E$$

$$\text{Bind } P E \alpha = \exists[ Op ]( P \alpha ( Op \alpha ) Op \times E ( Op \alpha ))$$

$$\quad -- \cong < P \times^P \text{Inner}^P P E \alpha >$$

$$\text{Embed} : E \rightarrow P$$

$$\text{Embed} = \text{Outer}^P$$
6.5. NOMINAL TYPES

\[
\text{data Rebind } (P_1 P_2 : \mathcal{P}) : \mathcal{P} \text{ where}
\]
\[
- \_ : \forall \{ \text{Op}_1 \text{Op}_2 \alpha \beta \}
\]
\[
\rightarrow P_1 \alpha \beta \text{Op}_1
\]
\[
\rightarrow P_2 (\text{Op}_1 \alpha) \beta \text{Op}_2
\]
\[
\rightarrow \text{Rebind } P_1 P_2 \alpha \beta (\text{Op}_2 \circ \text{Op}_1)
\]

\[
\text{Rec : } \mathcal{P} \rightarrow \mathcal{P}
\]
\[
\text{Rec } P \alpha \beta \text{Op} = P (\text{Op} \alpha) \beta \text{Op}
\]

**Open/close based interface** We have shown how the types provided by the library **Binders Unbound** can be expressed within our system. What about the operations? Their library generically provides the usual operations such as computing free variables, comparing two terms up to $\alpha$-equivalence, substitutions and performing a renaming. However in order to let the user program the remaining specific operations, the library had to commit to a particular implementation or interface to program with binders. They chose to provide an interface with a default implementation using Locally Nameless [Charguéraud, 2011, Aydemir et al., 2008]. We discussed at length in section 6.1 the limitations of an interface based on open and close (here called unbind and bind respectively). In particular when the type of abstractions is kept abstract the convenience is reduced when pattern matching, performance is hurt due to unwanted traversals, and structural recursion is no longer possible.

**Telescopes** Here is an example of the usefulness of the combinator **Rebind**, namely telescopes. Telescopes are widely used in dependently typed programming languages. A telescope is a sequence of typed bindings. Let $\Gamma$ be a meta-variable for such a telescope defined as $(A : \text{Set}) (x : A)$. Telescopes can be used to represent an environment in a typing judgement as in $\Gamma \vdash x : A$. They can be used to represent a sequence of arguments types as in $\Gamma \rightarrow A$. They can also be used to represent a sequence of typed arguments as in $\lambda \Gamma \rightarrow x$. While all these construction could be made by nesting **Bind**, this would tie the telescope to a particular usage. If we want the telescope to be a value on its own, its needs to be a pattern type. Hence the use of **Rebind** instead of **Bind**.

To illustrate **Rebind** and telescopes here are two mutually defined data types. The type **Exp** represents expressions in a small dependently typed language where types and expressions are fused in the same syntactic class. Expressions have variables, dependent function types, $\lambda$-abstractions, function applications, and a sort called **set**. The type **Tele** represents nested sequences of bindings associated with an expression, namely telescopes:
mutual
data Exp : E where
  V : Name E → E Exp
  Π : Bind Tele Exp → E Exp
  X : Bind Tele Exp → E Exp
  _·_ : Exp × E List E → E Exp
  set : 1 E → E Exp

data Tele : P where
  [] : 1 P → P Tele
  :: : Rebind (Binder P × P Embed Exp) Tele → P Tele

We show how to compute the free variables for expressions, lists of expressions, and telescopes. To do so we have to lift the function rm to telescopes as well:

mutual
  fv : Exp → E List E Name E
  fv (V x) = [ x ]
  fv (Π bind Γ t) = fvTele Γ ++ rmTele Γ (fv t)
  fv (X bind Γ t) = fvTele Γ ++ rmTele Γ (fv t)
  fv (_·_ (t , us)) = fv t ++ fvL us
  fv (set _) = []

fvL : List E Exp → E List E Name E
fvL [] = []
fvL (t :: ts) = fv t ++ fvL ts

fvTele : ∀ {α β Op} → Tele α β Op → List (Name α)
fvTele ([]) = []
fvTele (::((binder b , embed τ) , Γ)) = fv τ ++ rm b (fvTele Γ)

rmTele : ∀ {α β Op} → Tele α β Op → List (Name (Op α)) → List (Name α)
rmTele ([]) (neutral _) = id
rmTele (::((binder b , embed _) , Γ)) = rm b o rmTele Γ

Conclusion  In this section on nominal types we have shown the expressiveness of our system to define various families of data types. Through a lightweight embedded language we can support nominal signatures with multiple sorts and pattern types as in FreshML, Coml and Binders Unbound. Hence worlds are at least as expressive as these languages. Using our
embedded language to define data types is kept very light since the resulting
data types are not much different from those written directly. However the
expressiveness of worlds is also a weakness. Indeed generic programming as
done in BINDERS UNBOUND is greatly simplified by having a language of
combinators instead of our flexible use of worlds. To this end we advocate
to have both flexible worlds with a mechanized notion of $\alpha$-equivalence and
combinators to get generic programming. We have not studied enough how
to integrate data type generic programming since there are plenty of ways
to build universes in AGDA and meta-programming tools are promising but
still too young.

6.6 Related work

The difficulty of programming with, or reasoning about, names, binders, and
$\alpha$-equivalence has been known for a long time. It has recently received a lot
of attention, due in part to the POPLMARK challenge [Aydemir et al., 2005].
Despite this attention, the problem is still largely unsolved: according to
Guillemette and Monnier, for instance, “none of the existing representations
of bindings is suitable” [Guillemette and Monnier, 2008].

In the following, we review several systems that are intended to facilitate
the manipulation of names and binders. This review is not exhaustive: we
focus on relatively recent related work.

In particular we have already covered nominal systems such as FRESHML
[Shinwell et al., 2003], FRESH OCAML [Shinwell and Pitts, 2005], Caml [Pottier, 2006]; de Bruijn indices [de Bruijn, 1972]; systems based on well-scoped
and Hook, 1994, Bird and Paterson, 1999, Altenkirch and Reus, 1999]; dy-
namically stratified representations such as Locally Nameless [Charguéraud,
2011, Aydemir et al., 2008] and Locally Named [Pollack et al., 2011, Sato
and Pollack, 2010]; and BINDERS UNBOUND [Weirich et al., 2011] which is
internally based on Locally Nameless.

**FreshML and Pure FreshML** Pure FRESHML [Pottier, 2007] is built
on top of FRESHML. The semantics of FRESHML dictates that pattern
matching against a name abstraction silently replaces the bound atom with
a fresh atom. FRESHML guarantees that “name abstractions cannot be
broken”. However, FRESHML is unsafe: it is possible for a name to escape
its scope. Put another way, FRESHML is impure: name generation is an
observable side effect.

Pure FRESHML imposes additional static proof obligations, which ensure
that freshly created atoms do not escape their scope, and correspond to
Pitts’ *freshness condition for binders* [2006]. Because these proof obligations
are expressed in a specialized logic, they can be discharged automatically.
Because it is safe, Pure FRESHML can be implemented either using atoms (such as the original FRESHML) or using de Bruijn indices. This is an implementation choice, which the programmer need not know about.

In contrast with Pure FRESHML, the approach proposed in the present work does require certain runtime checks: the operation \( \text{exportTm} \) fails if its argument contains a free name that cannot be exported. We claim that often those checks are required and thus would be discharged by Pure FRESHML only with equivalent checks. However in some cases, some invariants of the code would make these checks redundant. Pure FRESHML might able to show that we can export without any check.

In Pure FRESHML, name abstraction is a primitive notion, and the fact that deconstructing an abstraction automatically freshens the bound atom is used to guarantee that all terms effectively live in a single world. In our work, in contrast, name abstraction is explained in terms of more basic notions, and it is possible to deconstruct a name abstraction without substituting a fresh name for the bound name. This leads to a finer-grained understanding of binding, and, in some cases, to greater runtime efficiency.

**Nominal System \( T \)** Pitts’ Nominal System \( T \) [2010] follows the tradition of FRESHML and guarantees that name abstractions cannot be violated. In order to ensure that names do not escape their scope, Pitts uses a dynamic technique: the \( \nu \) construct, which can be applied to any term, turns every name occurrence that is about to escape its scope into a harmless “anonymous name”, known as anon (or new). One potential advantage of this approach is that the application of \( \nu \) to a term can be lazily evaluated, whereas our \( \text{exportTm} \) operation requires eagerly traversing the entire term.

We can emulate this behavior in our system by adding a special value to the type for names to represent anon. We experimented with this option in our development [Pouillard, 2011a] by defining a type \( \text{Name?} \alpha \) as Maybe \( (\text{Name} \alpha) \) and anon as nothing. Most operations can be easily lifted. In particular \( \text{export?} \) gets the type \( \text{Name?} (b \triangleleft \alpha) \rightarrow \text{Name?} \alpha \) and so becomes “total”. Then, exporting terms gets the type \( \text{Tm} (b \triangleleft \alpha) \rightarrow \text{Tm} \alpha \). However there is no direct equivalent for \( \neg \text{Name?} \), since the empty world is indeed inhabited by anon. Instead we have that only anon inhabits the empty world.

One may wonder if the use of the Maybe type could be avoided? Indeed we tried another option in our development [Pouillard, 2011a] where the type \( \text{Name?} \alpha \) is equal to \( \text{Name} (\alpha \uparrow 1) \) and anon is equal to zero\(^3\). We also lifted most of the operations from \( \text{Name} \) to \( \text{Name?} \). We also gain “total” functions to export names and terms which would allow for a lazy exporting at the price of delaying “errors”.
A separate “data layer” Some systems are said to have a “data layer” separated from the “computation layer” for types. The data layer is generally a LF signature of a Logical Framework [Harper et al., 1993] (LF for short). This generally means that data types are only defined in the data layer. In the data layer there is an arrow type for functions but it should not be confused with computational functions that we expect from a programming language. A type constructor from the data layer can then be injected in the computation layer. The injection from the data to computation layer is a place where these systems differ. The data and computation layers being separated, this implies that we cannot mix first-class computational functions and data types.

In the case of a simply typed LF, we can map the data layer signatures to nominal signatures (section 6.5.1). To do so, we build an injection called \([\_]\) from LF types to atom sorts. Usually this means an atom sort per data sort. Then the translation called \([\_]\) of the signature is straightforward. The arrow case \([S \to T]\) is translated to \(<[S]\>_\delta [T]\). Finally for each data type \(\delta\), a data constructor is added for variables. This constructor has type: \(\forall \delta : \text{Name}^\delta \to \delta\). This translation can be used as an intuition of what it means to lift a type from the data layer to the computation layer and also as an initial step to support LF signatures in our system. In particular Licata and Harper follow a similar translation but using a single constructor for variables shared among the complete signature. Here is an example:

\[
\begin{align*}
\{ & \text{LF signature for System F:} \\
&Ty : \text{type.} \\
&arr : Ty \to Ty \to Ty. \\
&all : (Ty \to Ty) \to Ty. \\
\} \\
&Tm : \text{type.} \\
&app : Tm \to Tm \to Tm. \\
&lam : Ty \to (Tm \to Tm) \to Tm. \\
&App : Tm \to Ty \to Tm. \\
&Lam : (Ty \to Tm) \to Tm. \\
\}
\]

Only two type expressions appear on the left of an arrow. The injection \([\_]\) is thus defined as follow:

\[
[Ty] = vty \\
[Tm] = vtm
\]

Applying the previously mentioned translation we obtain the following data types:


\[
data \ Ty : \ E \ where
\]
\[
VTy : Name^e \ vty \mapsto^e Ty
\]
\[
arr : Ty \times^e Ty \mapsto^e Ty
\]
\[
all : < vty >^e Ty \mapsto^e Ty
\]

\[
data \ Tm : \ E \ where
\]
\[
VTm : Name^e \ vtm \mapsto^e Tm
\]
\[
app : Tm \times^e Tm \mapsto^e Tm
\]
\[
lam : Ty \times^e < vtm >^e Tm \mapsto^e Tm
\]
\[
App : Tm \times^e Ty \mapsto^e Tm
\]
\[
Lam : < vty >^e Tm \mapsto^e Tm
\]

**Elphin, Delphin, Beluga, Beluga\(\mu\)**  

Elphin [Schürrmann et al., 2005], Delphin [Poswolsky and Schürrmann, 2008, 2009], and Beluga [Pientka, 2008] are closely related to one another in several ways. They aim at building programming languages where data types are built from LF types and terms.

Elphin only has a limited way to include types from the data layer in the computation layer. Both Delphin and Beluga have contexts but their handling is different. Delphin deals with a “current context” while Beluga has explicit contexts. Delphin allows incremental changes of the current context using \(\nu\) whereas Beluga combines contexts and LF objects at the frontier of data and computation.

Beluga\(\mu\) [Cave and Pientka, 2012] extends Beluga with richer computational types. In Beluga\(\mu\) we can define data types in the computation layer as well. These data types can be recursive and indexed by LF objects of the data layer. While substitution comes for free at the data layer, substitution has to be user defined on data types from the computation layer. We think more connections between our system and Beluga\(\mu\) are to be found. We also notice their use of our system to prove properties of their language in Coq proof assistant. They used a simplified version of our 2010 paper [Pouillard and Pottier, 2010] which corresponds to the simplifications we have made in section 6.3.

At the data level, Elphin, Delphin, Beluga provide substitution and higher-order matching as primitive operations. This ambitious approach can eliminate some boilerplate code, at the cost of a complex meta-theory. By contrast, the meta-theory of our proposal is very simple, as it only extends an existing logical relations argument with a few new primitive types and operations. We argue that some of the boilerplate can still be eliminated via generic programming as this is done by Licata and Harper but also in Binders Unbound.
Licata and Harper’s system Licata and Harper [2009] aim to provide substitution for free when possible; and they expose the use of well-scoped de Bruijn indices to the programmer, whereas we offer a choice between nominal and de Bruijn-based representation techniques.

This said, there are numerous similarities between the two systems. Both keep track of the context, or world, within which each name makes sense. Both offer flexible ways of parameterizing or quantifying types over worlds. Both offer ways of moving data from one world to another: Licata and Harper’s weakening and strengthening respectively correspond to our import (coerce) and export operations. Both systems support first-class computational functions. Not all functions can be imported or exported, but some can: for instance, in both systems, the example of normalization by evaluation (section 3.4), which requires importing a function into a larger world, is made type-correct by planning ahead and making this function polymorphic with respect to an arbitrary world extension.

Distinctions One traditionally distinguishes several broad approaches to the problem of names and binders, which employ seemingly different tools, namely: atoms and atom abstractions; well-scoped de Bruijn indices; higher-order abstract syntax. We believe that this distinction can be superficial. In fact, our work presents strong connections with all three schools of thought. Perhaps more important are the following questions:

Can $\alpha$-equivalent terms be distinguished? Except for bare de Bruijn indices and plain nominal terms all the systems we have presented prevent $\alpha$-equivalent terms to be distinguished. These systems offer an adequate encoding of “nominal” terms and guarantees that the identity of a bound name cannot be observed.

What hygiene properties are enforced by the system? The base hygiene property is prevent from $\alpha$-equivalent terms to be distinguished. We now focus on more hygiene properties. In FreshML, Fresh OCAML, Caml, Locally Nameless, Locally Named, and Binders Unbound generating names is an observable effect. Said differently functions can turn $\alpha$-equivalent inputs into not $\alpha$-equivalent outputs. Nominal System T repairs this problem by dynamically detecting an atom that attempts to escape and by turning it into a harmless “anonymous atom”. Systems based on well-scoped de Bruijn indices enforce the invariant that every name is within range, that is, every name refers to some binding site. However, this alone does not imply that indices are correctly adjusted where needed, or that comparisons between names are allowed only when they make sense. In systems based on higher-order abstract syntax, and in Pure FreshML, name manipulation is hygienic by design: this is built in the syntax and semantics
of the programming language.

In the present document, hygiene is built in at a very low level. We provide a small number of abstract types, such as Binder and Name, together with a small number of operations. These operations are restricted on purpose: for instance, comparing two binders for equality is disallowed; comparing two names for equality is permitted only if they inhabit a common world. Through logical relations and parametricity, we are able to explore the consequences of these restrictions and to find out which hygiene properties can be expected of a well-typed program. In particular, we guarantee that two $\alpha$-equivalent terms cannot be distinguished and that functions turn $\alpha$-equivalent inputs into $\alpha$-equivalent outputs. These results hold because our definition of $\alpha$-equivalence is the logical relation, and that every well-typed program inhabits this relation. Moreover, our definition of $\alpha$-equivalence corresponds to the “standard” notion of $\alpha$-equivalence, at least for all nominal signatures like the type $\text{Tm}$.

**Is there a type for names that can be freely used in types?** The answer to this question is positive for most “first order” systems we have studied: de Bruijn indices, well-scoped de Bruijn indices, Locally Nameless, Locally Named, FRESHML, FRESH OCAML, Coml, Pure FRESHML, Nominal System $T$, BINDERS UNBOUND, and in the present work.

In systems based on LF and higher-order abstract syntax the type for names is not freely used. Instead, names inhabit all types issued from the data layer.

**Does the system have different data and computation layers?** Elphin, Delphin, Beluga, Beluga$^\mu$ clearly have two different layers. Since Coml does not support function while OCAML does we conclude that Coml has two different layers as well. In de Bruijn indices, well-scoped de Bruijn indices, Locally Nameless, Locally Named, FRESHML, FRESH OCAML, Pure FRESHML, Nominal System $T$, BINDERS UNBOUND and the present work there is no separation. However very few systems handle the mix of computational functions and data types with binders. Systems based on a generator or generic programming such as most Locally Nameless and Locally Named implementations, Coml, and BINDERS UNBOUND disallow types with computational functions. In Pure FRESHML, there is no support for first class functions at all. In de Bruijn indices, well-scoped de Bruijn indices, FRESHML and FRESH OCAML data and computation can be mixed since little operations are generically provided. However in FRESHML and FRESH OCAML the swap operation is generically provided and supports functions. In Licata and Harper’s work [2009] data and computation can be mixed. However they are both part of a “universe” which is then interpreted into computation types of the host language.
6.6. RELATED WORK

Is there a set of types where substitution can be defined? If so what are the restrictions? Some systems let the user program substitution functions. Some systems try to provide them for free either at all types or have restrictions. When a system has a specific “data layer” for types, the goal is to have substitution for free on these types once injected into the computation layer.

In Elphin, Delphin, and Beluga, substitution for data types comes for free but the data layer is restricted and cannot embed computational functions.

In Belugaβ there is substitution has to be defined for data types in the computation layer and comes for free on the data layer.

In FreshML, Fresh OCAML, Nominal System T, Pure FreshML this is up to the user to program substitution functions. In Coml (systems based on nominal signatures), Locally Nameless, Locally Named programmers have to define substitution functions but generators may be provided for usual cases. In Binders Unbound, substitution is generically provided for a family of types not including functions. In Licata and Harper’s work their is a generic definition for the substitution which is conditioned by criterion on the type.

In our system, substitution has to be programmed by the user and no particular set of types is prescribed for this task. Then as we have shown earlier a wide range of signatures can be embedded in our systems and generic programming could be applied on those.

How does the system keep track of the context or world in which a name makes sense? In Pure FreshML and in Nominal System T, there is effectively just one world, within which every name makes sense; static or dynamic checks guarantee that no confusion can arise. In Elphin, Delphin, or in Licata and Harper’s system, the meaning of types is relative to a “current context”, and a number of modalities are provided to discard the current context, extend it with one new name, etc. In Beluga and Belugaβ, contexts are explicit: a data layer type, once annotated with a context, becomes a computation layer type. In the present work, worlds are explicit, and are built into algebraic data type definitions by the programmer. There is no notion of a “current world”: multiple worlds can co-exist, and mechanisms are offered for transporting names (or whole data structures) from one world to another.

None of de Bruijn indices, Locally Nameless, Locally Named, FreshML, Fresh OCAML, Coml, or Binders Unbound keep track of the context in which a name makes sense.

Which high-level operations are involved in the semantics of the programming language? The semantics of the “nominal” systems (such as FreshML, Fresh OCAML, Coml, Pure FreshML, Nominal System T)
involves renaming. In Locally Nameless, Locally Named, and BINDERS UN-BOUND the open/close operations are costly and necessary to use to go under binders. The semantics of Elphin, Delphin, Beluga, and Beluga$\mu$ involve higher-order matching. In the present work, as well as in Licata and Harper’s work, no costly operations are built into the semantics; high-level operations, such as our import and export operations, are programmed explicitly or obtained via generic programming.

Moving across representations  It is arguably desirable to be able to offer several choices of representation within a single system, and to be able to migrate from one representation to another. Our system supports multiple representation styles, and combinations thereof (section 6.4). Furthermore, our implementation of normalization by evaluation (section 3.4) illustrates how to move back and forth between “syntactic” name abstractions and “semantic” name abstractions in the style of higher-order abstract syntax.

Robert Atkey and co-authors [Atkey, 2009, Atkey et al., 2009] investigate how to move back and forth between higher-order abstract syntax and de Bruijn indices. The translation out of higher-order abstract syntax produces well-scoped de Bruijn indices, but the proof of this fact is meta-theoretic. Atkey uses Kripke logical relations to argue that the current world at the time of application of a certain function must be larger than the world at the time of construction of this function. This seems somewhat related with our use of bounded polymorphism in the definition of semantic name abstractions (section 3.4). An exact connection remains to be investigated.
Chapter 7

Conclusion

7.1 Contributions

Our contributions are practical and fundamental. On the practical side, we have built a library (in Agda) for programming with names and binders. The library comprises a safe programming interface and a sound implementation, which has been mechanically proved against a strong specification. The interface supports different styles for binders: nominal, de Bruijn indices, de Bruijn levels, and combinations of them.

Our interface is not only safe but expressive as well. Explicit worlds enable both multiple kinds of variables and precise control over the scoping rules. Name abstraction is not a primitive type nor an abstract type but concretely built out of more atomic types. While expressive and safe, the system is economical on the number of introduced types.

On a fundamental side, we re-use the logical relations defined for Agda in [Bernardy et al., 2010], and build a logical relation argument which provides a strong specification of $\alpha$-equivalence by building a unified model. This is the very same model that is used for all styles: nominal, de Bruijn indices, de Bruijn levels and the combinations. The framework of logical relations provides a systematic way of defining $\alpha$-equivalence on complex data types. Moreover free-theorems arise for world-polymorphic functions defined by the user, yielding interesting properties about user code for free.

This work also establishes numerous connections between various systems of the three schools of thought (nominal, de Bruijn, HOAS). We built our library with a “nominal” insight and lightly integrated de Bruijn indices based on well-scoped de Bruijn indices approach. We then built a normalization by evaluation algorithm which shows how “syntactic” and “semantic” abstraction can be combined.

This unified approach does not stop here. De Bruijn levels, Locally Nameless, Locally Named, and combinations of them can be safely built on top of our abstract interface and programmed precisely. Through the
use of generic traversals and traversal kits, we can share most of the usual
definitions we have on terms.

Moreover our types are very flexible, as shown by the embedding of
nominal signatures, Coml types, and Binders Unbound types. Not only
flexible, our types automatically come with a definition for $\alpha$-equivalence
which is guaranteed to be preserved by the well-typed programs using our
interface.

7.2 Future work

As future work we would like to make our library lighter to use. To do so
we would like to infer most of the inclusion witnesses needed to move from
a world to another.

While hand-written generic traversals already avoid code duplication, we
would like to generically define this traversal for a fixed universe of types.

Studying how this system could support the presence of side-effects
would be an interesting direction as well. This could be done either by
considering a language design with our features and side effects or by study-
ing how our types compose with particular effects as monads.

Finally we would like to explore how convenient this technique is, to
not only program but reason about programs. Since the library is based on
abstract types, this would require exporting properties about the functions
of the interface. We can notice that this direction is promising since a
simplified version of our approach has been successfully used by Cave and
Pientka to prove properties of Beluga$\mu$.

We would also like to better study the connection with systems based on
LF and higher-order abstract syntax. A direction could be to combine the
universe from Licata and Harper but using our library instead of well-scoped
de Bruijn indices.

We also need to deal with a proper extraction of our library. We want
to erase: worlds, membership proofs, world inclusion witnesses, etc. A
real implementation should rely on machine integers; and useless traversal
functions (like $\text{coerceTm}$) should be optimized away.

We focused on names and binders to guarantee that the binding structure
of well-scoped terms is preserved by well-typed programs. However safe and
expressive meta-programming requires that not only scopes but types are
preserved. We worked on initial ideas in this direction but we left this to
future work.
Bibliography


Xavier Leroy, Damien Doligez, Jacques Garrigue, Didier Rn, and Jrme Vouillon. The Objective Caml system, October 2005. URL http://caml.inria.fr/.


# List of Figures

2.1 The NOMPA interface .............................................. 49
3.1 Lifting trName ................................................... 66
4.1 Logical relations for core types ................................. 83
4.2 Logical relations for data types ................................. 84
4.3 Relations for NOMPA types ....................................... 90
5.1 Core operations on names ....................................... 99
5.2 Operations on names ............................................. 99
5.3 New rules for world inclusion .................................. 100
5.4 Shifting versus adding example ............................... 110
5.5 Various term types: from concrete to abstract ............... 111
6.1 Various forms of name abstraction ............................ 127
Index

α-equivalent, 26

Abstract Syntax Trees, 20
algebraic data types, 30
assuming, 27
AST, 20

binder, 26
binding-links, 140
bound, 26

Code

\( \beta\)-red\(^p\), 108
\( \beta\)-red, 70, 147
\( \perp \), 37
\( \odot \)\-Kit, 68
\( \emptyset \), 55, 96
\( \equiv \), 38
\( \llbracket \cdot \rrbracket \), 169
N, 30
P, 159
\( \vdash \)Name\( \emptyset \), 53, 55, 96
\( \neg \)A, 38
\( \nu^* \), 152, 154
\( \subseteq \emptyset +1 \), 100
\( \subseteq \emptyset \), 54, 96
\( \subseteq \)Reasoning, 55
\( \subseteq \# \), 54
\( \subseteq \lhd \), 54
\( \subseteq \)dist\(-++\lhd \), 137
\( \subseteq \)dist\(-++1\lhd \), 137
\( \subseteq \)dist\(-\lhd +1 \), 137
\( \subseteq \)dist\(-\lhd + \), 137
\( \subseteq \)refl, 54, 96
\( \subseteq \)trans, 54, 55, 96
\( \top \), 37
\( \nu^* \), 152, 154

AbsPreTm, 126, 128
AbsTm, 121
Add\(^d\).kit, 137
Atom, 41, 120
Binder\(^{dp} \), 163
Binder\(^p \), 163
Binder, 50, 96
Bind, 164
Bool, 30
B, 85
Coerce, 67
Comm, 145
DataEnv, 61
DeBruijn, 142
Exp, 153, 154, 160, 165
Fin, 95, 100
FreshLink, 143
Fresh, 143
Inner\(^p \), 162
Let, 42, 140
Link, 140
List, 32
Name\(^{e} \), 157
Name, 50, 96
Neutral\(^{1*} \), 155, 157
Neutral\(^{2*} \), 155, 157
Neutral\(^* \), 155, 157
NomFresh, 143
Nom, 142
Outer\(^p \), 160, 162
Pat, 73, 161
PreTm, 126
Preserve\(\equiv \), 88
Program, 35
Rebind, 164
Rec, 164

185
RelatedFunctions, 81
RenameEnv^l, 135
SemAbs, 74, 75
Sem, 74
Set_0, 37
Set_1, 37
Sort, 155
SubstEnv+\subseteq, 128
SubstEnv^l, 135
SubstEnv, 65, 66
Supply, 65
SynAbs^D, 126
SynAbs^N, 74, 128
Tele, 165
Tm^A, 41, 121
Tm^D, 97
Tm^L\Rightarrow Tm^N, 138
Tm^L, 133
Tm^N, 94
Tm, 50, 140
TraversePreTm, 127
Tree, 34
V, 41, 94
World, 96
\_\_\_, 41, 133
\_\₊\_, 36
\_\_\_\_\_\_\_\_\_\_\_, 38
\_\_\_\_\_\_\_\_\_\_\_\_, 53, 96
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 152, 154
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 97, 98
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 98
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 31
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 36
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 55, 97
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 31
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 98
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 75
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 31
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 54, 79
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 39
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 54, 79
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 39
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 53
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 81
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 89, 92
INDEX

187

<_,_>, 159, 164
addTm\^D, 107
addTm\^L, 138
add\^D, 98
add\^N, 101
appTm\^D, 104
appTm\^N, 95
ba, 44, 47
binder\^N, 52
closeTm?, 70
closeTm\^D?, 107
closeTm\^L, 136
closeTm, 121, 127, 129
cmp=ba, 44, 47
cmpName\^↑, 108
cmpTm\^D, 109
cmpTm\^L, 133
cmpTm, 63, 88
cmp\^N, 100
coeTm, 64
coeceEnv, 76
coeceKit, 64
coeceTm\^L, 138
coeceTm, 70
coece\^N, 53, 55, 79, 96
commEnv, 145
compTm\^D, 104
convTm\^N\-emptyset\Rightarrow Tm\^N\-emptyset, 139
convTm\^N\-emptyset\Rightarrow Tm\^L, 139
conv, 71
env-length-Tm\^D, 48
eval, 75
exportWith, 60
export\^N?, 57, 79
export\^N, 56
extEnv, 63, 71
extendNameCmp, 62
extend, 60
falseTm, 52
false, 30, 85
fast-fv, 48
fa, 125
filter, 33
fv\^D, 104
fv, 43, 44, 47, 61, 133, 140, 148,
153, 154
idTm\^D, 104
idTm, 52
id, 32
importFun, 145
init, 143
is42?, 85
kitVar, 146
lam, 154, 160
length, 33
let\^′, 122, 161
lookup, 61
mapKit, 68
map, 33
match, 161
nameOf, 140
name\^B, 52, 79
next, 143
node, 34
nomview, 150
not, 30
occurs, 60
occ, 60
openSubstTm, 122, 127, 128
openTm, 121, 150
plug, 73
pred\^N?, 102
print, 36
protect\^↑A, 106
protect\^↑, 103
protect\^↓↑, 149
protectedAdd\^↑, 113
protectedAdd, 112
pure, 40, 67
reify, 76
renameAKit\^L, 136
renameAKit, 67
renameKit\^+\subseteq, 128
renameKit, 66
renameTm?, 70
renameTm\^P?, 106
renameTm\^P\^A, 106
renameTm\^D, 106
renameTmL⇒TmR, 139
tenameTmL?, 136
renameTmL'A, 136
renameTmL, 136
renameTm, 146
ren, 149
rerootTmL', 138
rm0, 104
rmA, 43
rm, 59, 140
seed, 65
set, 165
shiftName', 103
shiftName, 102
shiftTmR, 107
show, 36
size, 51, 123, 124
starKit, 68
strengthen?, 140
substKit, 67
substPreTm, 128
substTmR, 108
substTmL', 136
substTm, 70, 147
substVarTmR, 108
subtractTmR?, 107
subtractTmR, 107
subtractTmL', 138
subtractR?, 102
subtractR, 100
subtractR', 101
suc#, 54, 79
sucR, 51, 96
sucR', 101
sucN', 101
sucN, 101
sucR', 65
suc, 30
sumForest, 34
sumTree, 34
t', 43
tR, 43
tY, 43
trAtom, 71
trBinder, 63
trName, 63, 65, 145
trTm', 69
trTmR', 105
trTm, 68
triple, 31
trueTm, 53, 55, 56
true, 30, 85
unprotectedAdd, 113
vr, 154
weakenTm, 147
weaken, 140
zeroR, 51, 96
zeroN, 98
zeroR', 65
zero, 30
[], 32
χ', 122
χ, 41, 94, 95
complete, 17
countext, 26
data constructors, 30
definitional equality, 38
definitionally equal, 38
equal pointwise, 39
expression types, 152
free, 26
fresh, 26
GADT, 30
has type, 18
higher-order, 33
inductive families, 29
infix, 16
inner, 159, 160
Keyword
...**, 34
Set, 37
with, 33
lexing, 19
links, 140
locally closed, 120
Locally Named, 120
Locally Nameless, 120, 126

mutually recursive, 34

name, 26
nominal, 27
nominal signatures, 152
Nominal terms, 152

occurrence, 26
outer, 159, 160

parsing, 20
pattern, 151
pattern type, 159
pattern types, 152
pattern matching, 30
pattern types, 152, 159
pointwise equality, 40
polymorphism, 32
propositional equality, 38

recursive, 30
regular tree types, 29

sequenced, 14
sound, 17
sum and product types, 29

tail, 33
token class, 20
tokens, 20
traversal kit, 63
types, 17
typing judgements, 18

variable, 26

wildcard, 33